

CERIO Corporation

CS-2424G-24PA5

PoE CS-2000 Series - 24 Port 10/100/1000M Gigabit Web Managed PoE+ Switch with 4 Combo Gigabit Ports (450Watt Power)



User Manual

Default IP / Login Information

IP Address	192.168.2.200
User Name	root
Password	default

V1.0a





FCC Warning

This device has been tested and found to comply with limits for a Class A digital device, pursuant to Part 2 and 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiates radio frequency energy and, if not installed and used in accordance with the user's manual, may cause interference in which case user will be required to correct the interference at his own expense.

CE Mark Warning

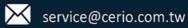
This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user many be required to take adequate measures.





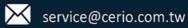


1.	Exterior		8
	1.1 Front	Panel	8
	1.2 Rear l	Panel Layout	8
2.	Software Co	onfiguration	9
	2.1 Exam	ple of Segment: (Windows OS)	9
	2.2 System	m login information and IP / Gateway Setting instructions	12
3.	Status		14
	3.1 System	m Information	14
	3.2 Loggi	ng Message	16
	3.3 Port		17
	3.3.1	Statistics	
	3.3.2	Error Disabled	
	3.3.3	Bandwidth Utilization	
	3.4 Link A	Aggregation	20
	3.5 MAC	Address Table	21
4.	Network		23
	4.1 DNS		23
	4.2 Host.		25
	4.3 System	m Time	26
5.	Port		29
	5.1 Port s	setting	29
	5.2 Error	Disabled	
	5.3 Link A	Aggregation	32
	5.3.1	Group Configuration	
	5.3.2	Port Setting	
	5.3.3	LACP	
	5.4 EEE		
	5.5 Jumb	o Frame	
6.	POE		
	6.1 POE P	Port Setting	
	6.2 POE P	Port Time Setting	41
7.	VLAN		42
	7.1 VLAN		42
	7.1.1	Create VLAN	
	7.1.2	VLAN Configuration	
	7.1.3	Membership	
	7.1.4	Port Setting	
	7.2 Voice	VLAN	48
	7.2.1	Property	



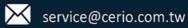


		7.2.2 Voice OUI	
	7.3	Protocol VLAN	51
		7.3.1 Protocol Group	
		7.3.2 Group Binding	
	7.4	MAC VLAN	53
		7.4.1 MAC Group	
		7.4.2 Group Binding	
	7.5	Surveillance VLAN	56
		7.5.1 Property	
		7.5.2 Surveillance OUI	
	7.6	GVRP	59
		7.6.1 Property	
		7.6.2 Member ship	61
8.	MA	C Address Table	65
	8.1	Dynamic Address	65
	8.2	Static Address	66
	8.3	Filtering Address	67
	8.4	Port Security Address	68
9.	Spa	nning Tree	69
	9.1	Property	69
	9.2	Port Setting	71
	9.3	MST Instance	73
	9.4	MST Port Setting	75
	9.5	Statistics	78
10.	Disc	covery(LLDP)	80
	10.1	Property	80
	10.2	Port Setting	81
	10.3	MED Network Policy	83
	10.4	MED Port Setting	85
	10.5	Packet View	87
	10.6	Local Information	89
	10.7	Neighbor	95
	10.8	Statistics	98
11.	DHO	CP	
	11.1	Property	100
	11.2	IP Pool Setting	101
	11.3	VLAN IF Address Group Setting	104
	11.4	Client List	105
	11.5	Client Static Binding Table	106



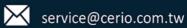


12.	Multicast		
	12.1 Genera	al	
	12.1.1	Property	
	12.1.2	Group Address	
	12.1.3	Router Port	
	12.1.4	Forward All	
	12.1.5	Throttling	
	12.1.6	Filtering Profile	
	12.1.7	Filtering Binding	
	12.2 IGMP	Snooping	
	12.2.1	Property	
	12.2.2	Querier	
	12.2.3	Statistics	
	12.3 MLD S	nooping	
	12.3.1	Property	
	12.3.2	Statistics	
	12.4 MVR		
	12.4.1	Property	
	12.4.2	Port Setting	
	12.4.3	Group Address	
13.	IP Configura	tion	
	13.1 IPv4 M	lanagement and Interfaces	
	13.1.1	IPv4 Interface & Default IP Configure	
	13.1.2	IPv4 Routes & Default Route Configure	
	13.1.3	ARP	
		lanagement and Interfaces	
	-	IPv6 Interface	
	13.2.2	IPv6 Addresses	
	13.2.3	IPv6 Routers	
	13.2.4	IPv6 Neighbors	
14.	-		
		S	
		S+	
	14.3.1	Method List	
	14.3.2	Login Authentication	
	-	gement Access	
	14.4.1	Management Service	
	14.4.2	Management ACL	





	14.4.3	3 Management ACE	
	14.5 Aut	hentication Manager	170
	14.5.1	1 Property	170
	14.5.2	2 Port Setting	
	14.5.3	3 MAC-Based Local Account	
	14.5.4	4 WEB-Based Local Account	
	14.5.5	5 Sessions	
	14.6 Port	t Security	
	14.7 Prot	tected Port	
	14.8 Stor	rm Control	
	14.9 DoS	5	192
	14.9.1	1 Property	
	14.9.2	2 Port Setting	
	14.10 Dyn	namic ARP Inspection	195
	14.10	0.1 Property	
	14.10	0.2 Statistics	
	14.11 DHC	CP Snooping	199
	14.11	1 Property	
	14.11	.2 Statistics	
	14.11	L.3 Option82 Property	202
	14.11	.4 Option82 Circuit ID	203
	14.12 IP S	ource Guard	205
	14.12	2.1 Port Setting	205
	14.12	2.2 IMPV Binding	
	14.12	2.3 Save Databases	
15.	ACL		210
	15.1 MA	C ACL	210
	15.2 MA	С АСЕ	211
	15.3 IPv4	4 ACL	214
	15.4 IPv4	4 ACE	214
	15.5 IPv6	6 ACL	219
	15.6 IPv6	6 ACE	220
	15.7 ACL	Binding	224
16.	QoS		226
	16.1 Prop	perty	226
	16.2 Que	eue Scheduling	229
	16.3 CoS	Mapping	230
	16.4 DSC	CP Mapping	232
	16.5 IP P	Precedence to Queue Mapping	234





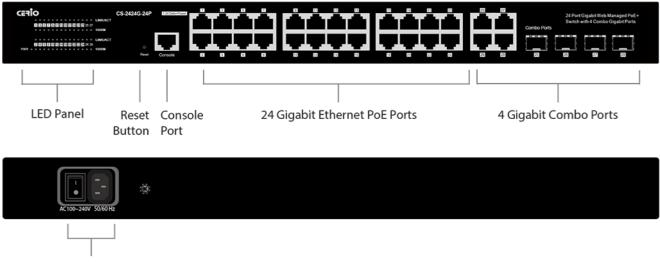
	16.6 Rate Li	mit	236
	16.6.1	Ingress / Egress Port	
	16.6.2	Egress Queue	
17.	Diagnostics .		240
	17.1 Loggin	g	240
	17.1.1	Property	
	17.1.2	Remote Server	
	17.2 Mirror	ing	244
	17.3 Ping		246
	17.4 Tracero	oute	247
	17.5 Coppe	r Test	248
	17.6 Fiber N	Aodule	249
	17.7 UDLD.		250
	17.7.1	Property	250
	17.7.2	Neighbor	
18.	Managemen	t	254
	18.1 User A	ccount	254
	18.2 Firmwa	are	255
	18.2.1	Upgrade / Backup	255
	18.2.2	Active Image	
	18.3 Config	uration	258
	18.3.1	Upgrade / Backup	258
	18.3.2	Save Configuration	
	18.4 SNMP		262
	18.4.1	View	
	18.4.2	Group	
	18.4.3	Community	
	18.4.4	User	
	18.4.5	Engine ID	
	18.4.6	Trap Event	
	18.4.7	Notification	
		l	
	18.5.1	Statistics	
	18.5.2	History	
	18.5.3	Event	
	18.5.4	Alarm	

+(886) 2-8911-6160



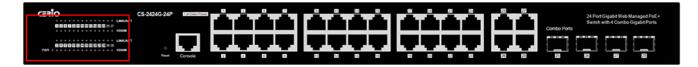
1. Exterior

1.1 **Front Panel**



Power Cord Input

1.2 **Rear Panel Layout**



Status LED lights for 24 Port 10/100/1000Mps with 4 Gigabit Combo Ports

Per Port: Link/Activity Status Per Port: 1000M/Gigabit Status Gigabit Combo Port : Link/Activity Status Gigabit Combo Port: 1000M/Gigabit Status Per Unit : PWR



- 1) AC Power On/Off Control Switch
- 2) AC input (100-240V/AC, 50-60Hz) UL Safety





2. Software Configuration

CS-2424G-24P A5 supports web-based configuration. Upon the completion of hardware installation, The Switch can be configured through a PC/NB by using its web browser such as Internet Explorer 6.0 or later.

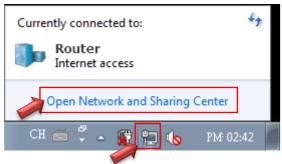
Set the IP segment of the administrator's computer to be in the same range as CS-2424G-24P A5 for accessing the system. Do not duplicate the IP Address used here with IP Address of CS-2424G-24P A5 or any other device within the network. Please refer to the following steps

Example of Segment: (Windows OS) 2.1

Step 1:

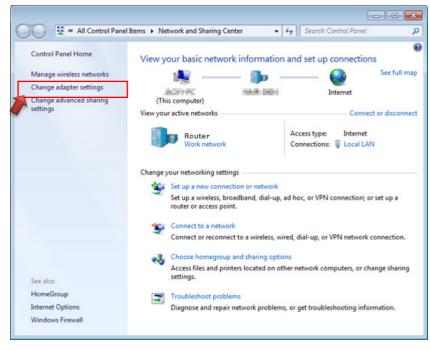
Please click on the computer icon in the bottom right window, and click "Open Network and Sharing

Center"



Step 2 :

In the Network and Sharing Center page, click on the left side of "Change adapter setting" button



+(886) 2-8911-6160





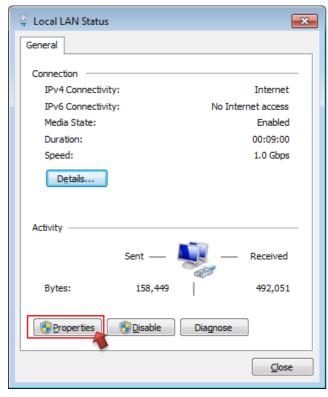
Step 3 :

In "Change adapter setting" Page, right click on Local LAN then select "Properties"



Step 4 :

In the "Properties" page, click the "Properties" button to open TCP/IP setting

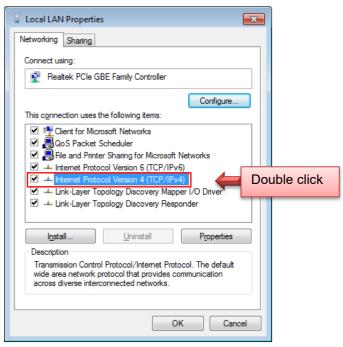






Step 5 :

In Properties page for setting IP addresses, find "Internet Protocol Version 4 (TCP/IPv4)" and double click to open TCP/IPv4 Properties window



Step 6:

Select "Use the following IP address", and fix in IP Address to: 192.168.2.X

ex. The X is any number from 1 to 253

Subnet mask : 255.255.255.0

And Click "OK" to complete fixing the computer IP settings

Internet Protocol Version 4 (TCP/IPv4)	Properties ?
General	
You can get IP settings assigned autorr this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatical	у
Ose the following IP address:	
IP address:	192.168.2.100
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
Default gateway:	
Obtain DNS server address autom	atically
Outer bits server address address	,
Preferred DNS server:	
Alternate DNS server:	· · ·
Valjdate settings upon exit	Ad <u>v</u> anced
	OK Cancel





Step 7:

Open Web Browser

Without a valid certificate, users may encounter the following problem in IE7 when they try to access system's WMI (http://192.168.2.200). There will be a "Certificate Error", because the browser treats system as an illegal website.

CERIO	24 Por	t Gigabit Managed PoE+ Switch	CS-2424G-24P with 4 Combo Gigabit Ports
		Login	
	Username:	root	
	Password:		
		Login 20	

System login Overview page will appear after successful login.

System login information and IP / Gateway Setting instructions 2.2

The CS-2424G-24P A5 web switch default IP is 192.168.2.200 Into the management page as follows, please enter Username and password

- Default IP Address: 192.168.2.200 \geq
- **Default Username and Password**

Management Account	Root Account
Username	root
Password	default

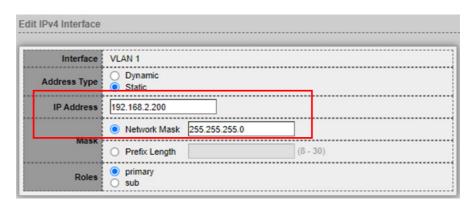
After the authentication procedure, the home page will show up. Select one of the configurations by clicking the icon.







Default IP Configure:



If you want to change the default IP (VLAN IP) address of the POE switch, Note please refer to the chapter : 13.1.1. for " IP Configuration > IPv4 Interface & Default IP Configure >" (Please refer to page 133)

Default Route Configure: (This function is the same as the "Default Gateway **Configure " of the POE switch)**

IP /	Address	0.0.0.0]		
	Mack	Network Mask	0.0.0.0]
	Mask	O Prefix Length				(0 - 32)
Next Hop Router IP	Address	192.168.2.254]		
	Metric	1		(1 - 255, d	efault 1)	

Note	If you want to make default Route IP address of the POE switch, please refer to the chapter : 13.1.2. for "IP Configuration > Pv4 Routes & Default Route Configure >" (Please refer to page 137)
------	--





3. Status

3.1 **System Information**

Administrator can check this page shows switch panel, CPU utilization, Memory utilization and other system current information. It also allows user to edit some system information.

squares indicate the port link is down. Below the switch panel, you can find a common Note

Status								
System Information Logging Message Port Link Aggregation MAC Address Table		1 3 5 7 9 11 13 1 2 4 6 8 10 12 14 1			25	26 27	28	
letwork								
Port				4000/				
OE Setting	System Information		Edit	100%				c
/LAN		00 04040 045	Lon	80%				
AC Address Table	Model	CS-2424G-24P		70%				
panning Tree	System Name	Switch		60%				
iscovery	System Location	default		50%				
нср	System Contact			40%				
lulticast				30%		4		
^o Configuration		8C:4D:EA:30:DA:3D		20%		- Ann		
ecurity	IPv4 Address	192.168.101.89		10%			AAA.	
CL		0 day, 0 hr, 6 min and 12 sec		0%				
20S		2023-01-01 08:05:12 UTC+8			13:10:00	13:11:00 Tim	13:12:00	13:13
Diagnostics	Current Time	2023-01-01-00.03.12 010-0	······			1117	e	
lanagement	Loader Version	3.6.7.55090		100%				
		Sep 07 2022 - 10:08:06		90%				M
				80%				
				70%				
	Firmware Date	Feb 08 2023 - 09:43:53		60%				
			,	50%				
	Telnet	Disabled		40%				
	SSH	Disabled		30%				
	нттр	Enabled		20%				
	HTTPS	Disabled		10%				
	SNMP	Disabled		0%	13:10:00	13:11:00	13:12:00	13:13:

Field	Description
Model	Model name of the switch.
System Name	System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" or "Switch#")
System Location	Location information of the switch.
System Contact	Contact information of the switch.
MAC Address	Base MAC address of the switch.





IPv4 Address	Current system IPv4 address.					
IPv6 Address	Current system IPv6 address.					
System OID	SNMP system object ID.					
System Uptime	Total elapsed time from booting.					
Current Time	Current system time.					
Loader Version	Boot loader image version.					
Loader Date	Boot loader image build date.					
Firmware Version	Current running firmware image version.					
Firmware Date	Current running firmware image build date.					
Telnet	Current Telnet service enable/disable state.					
SSH	Current SSH service enable/disable state.					
нттр	Current HTTP service enable/disable state.					
нттрѕ	Current HTTPS service enable/disable state.					
SNMP	Current SNMP service enable/disable state.					

Edit System Information

Administrator can click "Edit" button on the table title to edit following system information.

System Name	Switch
System Location	default
System Contact	default

- System Name: System name of the switch. This name will also use as CLI prefix of each line. ("Switch>" \geq or "Switch#").
- System Location: Location Location information of the switch. \geq





 \triangleright System Contact: Contact information of the switch.

Click the "Apply" button to save your changes or "Close" the button to close settings.

Logging Message 3.2

Administrator can use this tools page to Inspection of system RAM and Flash status.

Status Logging Messa	ige				
System Information Logging Message Port Link Aggregation MAC Address Table	Viewing F	Message Table		Showing 1 to 5 of 5 entries	٩
	Log ID	Time	Severity	Description	
≉ Port	1	Jan 01 2023 08:00:28	notice	AAA-0-CONNECT: New http connection for user root,	source 192.168.101
✤ POE Setting	2	Jan 01 2023 08:00:14	notice	PORT-5-LINK_UP: Interface GigabitEthernet25 link up	0
* VLAN	3	Jan 01 2023 08:00:13	notice	PORT-5-LINK_UP: Interface VLAN1 link up	
MAC Address Table	4	Jan 01 2023 08:00:13	notice	PORT-5-LINK_UP: Interface GigabitEthernet27 link up	0
 Spanning Tree 	5	Jan 01 2023 00:00:13	notice	SYSTEM-5-COLDSTART: Cold startup	
DiscoveryDHCP) [Defect]			First Previous
	Clear	Refresh			First Prev

- \geq Viewing: The logging view including:
 - **RAM:** Show the logging messages stored on the RAM.
 - Flash: Show the logging messages stored on the Flash.

Field	Description
Log ID	The log identifier.
Time	The time stamp for the logging message.
Severity	The severity for the logging message.
Description	The description of logging message.

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.





3.3 Port

Display detailed port summary and status information for each port.

3.3.1 **Statistics**

Administration can choose to view displays standard counters on network traffic form the Interfaces, Ethernet-like and RMON MIB. Interfaces and Ethernet-like counters display errors on the traffic passing through each port. RMON counters provide a total count of different frame types and sizes passing through each port. The "Clear" button will clear MIB counter of current selected port.

Status → Port → Statistics – Status	
System Information Logging Message	Port GE1 V
Statistics Error Disabled Bandwidth Utilization	MIB Counter C Interface C Etherlike C RMON
Link Aggregation MAC Address Table Network	Refresh Rate
✓ Port	○ 30 sec
POE Setting	Clear
* VLAN	
MAC Address Table	Interface
 Spanning Tree 	ifInOctets 0
✤ Discovery	ifInUcastPkts 0
* DHCP	ifInNUcastPkts 0
✤ Multicast	
 IP Configuration 	ifInDiscards 0
	ifOutOctets 0
* ACL	ifOutUcastPkts 0
¥ QoS	ifOutNUcastPkts 0
 Diagnostics 	ifOutDiscards 0
 Management 	

Click the "Clear" button to clear this page.





Interface	
ifInOctets	1226044
ifInUcastPkts	8677
ifInNUcastPkts	343
ifInDiscards	0
ifOutOctets	2813449
ifOutUcastPkts	5587
ifOutNUcastPkts	194
ifOutDiscards	0
ifInMulticastPkts	226
ifInBroadcastPkts	117
ifOutMulticastPkts	194
ifOutBroadcastPkts	0

Etherlike	
dot3 StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3 Stats SingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3 Stats SymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

RMON	
etherStatsDropEvents	0
etherStatsOctets	1236728
etherStatsPkts	9117
etherStatsBroadcastPkts	117
etherStatsMulticastPkts	226
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	6502
etherStatsPkts65to127Octets	1080
etherStatsPkts128to255Octets	122
etherStatsPkts256to511Octets	1251
etherStatsPkts512to1023Octets	150
etherStatsPkts1024to1518Octets	12





- \geq Port : Select one port to show counter statistics.
- \geq **MIB Counter :** Select the MIB counter to show different counter type.
 - All : All counters.
 - Interface : Interface related MIB counters.
 - Etherlike : Ethernet-like related MIB counters.
 - **RMON :** RMON related MIB counters.
- \geq Refresh Rate : Refresh the web page every period of "None, 5 sec, 10 sec, 30 sec "seconds base to get new counter of specified port.

3.3.2 **Error Disabled**

If administrator has set Error disabled functions then can monitor information in page.

Status Port 🔿 Error Disa	abled				
- Status System Information	Erro	r Diaa	bled Tab	la	
Logging Message	EIIO	DISa	bieu iau	ne	
					9
Statistics					
Error Disabled		Port	Reason	Time Left (sec)	
Bandwidth Utilization		GE1			
Link Aggregation		GE2			
MAC Address Table		GE3			
✤ Port	U	GE4			
✤ POE Setting		GE5			
VLAN		GE6			
* VLAN		GE7			

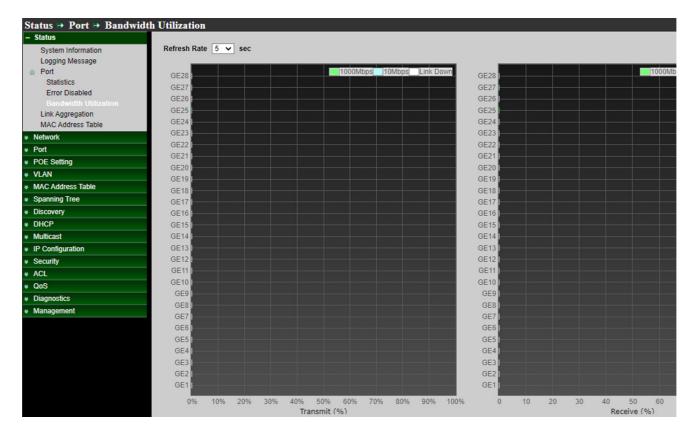
Field	Description
Port	Interface or port number.
Reason	 Port will be disabled by one of the following error reason: BPDU Guard. UDLD. Self Loop. Broadcast Flood. Unknown Multicast Flood. Unicast Flood. ACL. Port Security Violation. DHCP rate limit. ARP rate limit.
Time Left (sec)	The time left in second for the error recovery.





Bandwidth Utilization 3.3.3

This page can display Tx / Rx Real-time bandwidth information of each port. (Instant used rate per port and this page will refresh automatically in every refresh period)



- \succ **Refresh Rate:** Refresh the web page every period of seconds to get new bandwidth utilization Rata.
 - **2**: Select the 2 second cycle from the drop-down menu to refresh the display page.
 - **5**: Select the 5 second cycle from the drop-down menu to refresh the display page. •

10: Select the 10 second cycle from the drop-down menu to refresh the display page.

3.4 **Link Aggregation**

If administrator has set LACP function then this can display LACP information. This system have support 8 Link Aggregation group. Administrator can enable 8 LAG.





- Status						
System Information	Link	Aggrega	ation T	able		
Logging Message Port Statistics						Q
Error Disabled	LA	G Name	Туре	Link Status	Active Member	Inactive Member
Bandwidth Utilization	LAG	1				
Link Aggregation MAC Address Table	LAG	_				
Network	LAG	-				
Port	LAG	4				
POE Setting	LAG	5				
VLAN	LAG	6				
MAC Address Table	LAG	7				
Spanning Tree	LAG	8				

Field	Description
LAG	LAG Name.
Name	LAG port description.
Туре	 The type of the LAG. Static: The group of ports assigned to a static LAG are always active members. LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

3.5 **MAC Address Table**

The MAC address table page displays all MAC address entries on the switch including static MAC address created by administrator or auto learned from hardware.

The "Clear" button will clear all dynamic entries and "Refresh" button will retrieve latest MAC address entries and show them on page.





Status → MAC Address Ta – Status	DIe				
System Information	MAC Ad	ddress Table			
Sector Port ■ Port	Showing	All 🗸 entries			Showing 1 to 23 of 23 entries
Statistics	30.431	MAC Address	Tree	Dest.	
Error Disabled Bandwidth Utilization	VLAN 1	8C:4D:EA:30:DD:53	Туре	CPU	
Link Aggregation		00:08:9B:D5:33:E4	Management	GE27	
MAC Address Table	1		Dynamic		
ℽ Network	1	00:11:32:11:76:30	Dynamic	GE27	
∗ Port	1	00:1A:97:01:AD:B1	Dynamic	GE27	
POE Setting	1	00:60:B9:BF:B6:74	Dynamic	GE27	
* VLAN	1	00:E0:A0:10:04:6C	Dynamic	GE27	
* MAC Address Table	1	10:60:4B:8B:78:99	Dynamic	GE27	
Spanning Tree	1	1C:6F:65:26:B9:13	Dynamic	GE27	
* Discovery	1	1C:6F:65:41:52:73	Dynamic	GE27	
* DHCP	1	40:B0:34:54:97:82	Dynamic	GE25	
* Multicast	1	58:38:79:0D:1C:12	Dynamic	GE27	
* IP Configuration	1	6C:B1:58:2E:38:67	Dynamic	GE27	
* Security	1	6C:B1:58:2E:38:74	Dynamic	GE27	
× ACL	1	6C:B1:58:2E:3B:35	Dynamic	GE27	
* QoS	1	6C:F0:49:0A:85:C1	Dynamic	GE27	
* Diagnostics	1	8C:4D:EA:04:F8:50	Dynamic	GE27	
✓ Management	1	90:09:D0:25:A9:4F	Dynamic	GE27	
-	1	94:DE:80:70:B4:CD	Dynamic	GE27	
	1	98:97:CC:3A:6A:0C	Dynamic	GE27	
	1	A4:5D:36:C7:4D:B3	Dynamic	GE27	
	1	E0:2A:82:A2:2D:40	Dynamic	GE27	
	1	F4:6D:2F:96:C8:77	Dynamic	GE27	
		F4:6D:2F:96:C8:77		GE27 GE27	
	1	F4.0D(2F(96)CC(7F	Dynamic	GEZI	

Field	Description			
VLAN	VLAN ID of the mac address			
MAC Address	MAC address			
	The type of MAC address			
	 Management: DUT's base mac address for management 			
Туре	purpose			
<i>,</i> ,	 Static: Manually configured by administrator 			
	 Dynamic: Auto learned by hardware 			
	The type of Port			
Port	 CPU: DUT's CPU port for management purpose 			
	Other: Normal switch port			

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.





4. Network

4.1 DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Use the DNS screen to configure and view the default DNS servers on the Switch. Use these pages to configure information about which DNS servers your network uses and how the switch operates as a DNS client.

DNS service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

You can use these pages to configure information about DNS servers the network uses and how the switch operates as a DNS client.

Network → DNS			
* Status			
– Network	DNS Configuratio	n	
DNS			
Hosts	DNC Control	O Disable	
System Time	DNS Statu	s 💿 Enable	
♦ Port	DNS Default Nam	e cerio.co.tw	(1 to 255 alphanumeric characters)
 POE Setting 	Divis Delauri Main	e centre.co.tw	
* VLAN	(Apply)		
MAC Address Table	Apply		
Spanning Tree	DNS Server Confi	guration	
* Discovery		<u> </u>	
* DHCP			Q
✤ Multicast	Destauras 1	DNS Server	
✤ IP Configuration			
* Security	1 19.	2.168.101.100	
* ACL	Add De	lete	

Use this page to configure global DNS settings and DNS server information.

DNS Configuration

Select the Disable or Enable button to specify whether to disable or enable the administrative state of the DNS client:

- \geq **DNS Status:**
 - **Disable :** Prevent the switch from sending DNS queries.
 - **Enable :** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name.
- \geq DNS Default Name : Enter the default DNS domain name to include in DNS queries.

+(886) 2-8911-6160





Note name must not be longer than 255 alphanumeeric characters.

Click the "Apply" button to save your changes.

DNS Server Configuration

Administrator can configure this DNS Server Setting "add" and " Delete " function management.

Field	Description
Preference	The Preference field displays the server preference order. The preference is set in the order in which preferences were entered.
DNS Server	Shows the server is added to the list.

Note which they were entered. You can specify up to eight DNS servers.

- \geq Add : To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the DNS Server Address and click Add. The server appears in the list below. You can specify up to eight DNS servers. The preference is set in the order created.
- \geq **Delete** : To remove a DNS server from the list, select the check box next to the server you want to remove and click Delete. If no DNS server is specified, the check box is global and will delete all the DNS servers listed.

Administrator can configure this DNS Server Configuration "Apply" and " Cancel "on the screen and reset the data on the screen to the latest value of the switch.





4.2 Host

This page provide administrator to view Host Name to IP Address Information, Administrator can set this page to manually map host names to IP addresses or to view dynamic host mappings.

Network 🗃 Hosts		
– Network	DNS Host Configuration	
DNS		
Hosts		Q
System Time	Host IPv4/IPv6 Address	
≽ Port		
✤ POE Setting		
* VLAN	cerio.cc 97.74.109.10	
 MAC Address Table 	Add Delete	
✤ Discovery	Dynamic Host Mapping	
¥ DHCP		
≽ Multicast		Q
✤ IP Configuration	Host Total Elapsed Type IPv4/IPv6 Address	
¥ ACL	0 results found.	
¥ QoS	Clear	

Click the "Clear" button to clear this page

DNS Host Configuration

Administrator can configure "add" and " Delete " for a static entry to the local dynamic host mapping Table function management.

ield	Description
lost	Show "host name" that for you assign to the specified IP address.
Pv4/IPv6 Address	The IP address associated with the "host name".
Pv4/IPv6 Address	The IP address associated with the "host name".
Add Host	
-	google.com (1 to 255 alphanumeric characters

- Host: Administrator can set the Host Name field, specify the static host name to add. \geq
- \geq IPv4/IPv6 Address: Enter the IP address to associate with the host name to this " IPv4/IPv6 Address" field, The entry is displayed in the list on the page after "Apply" creation.



For Host Name field, Must be follow 1 to 255 alphanumeric characters, Its length cannot

Click the "Apply" button to save your changes or "Close" the button to close settings.

Dynamic Host Mapping

Administrator can clear all the dynamic host name entries from the list, click the Clear button.

The Dynamic Host Mapping table shows host name-to-IP address entries that the switch learned.

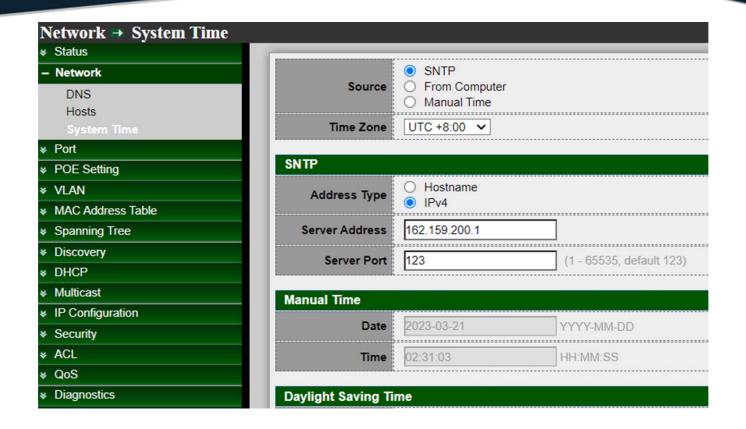
Field	Description
Host	Displays the lists the host name you assign to the specified IP address.
Total	Displays the amount of time since the dynamic entry was first added to the table.
Elapsed	Displays the amount of time since the dynamic entry was last updated.
Туре	Displays the type of the dynamic entry.
IPv4/IPv6 Address	Displays the lists the IPv4 or IPv6 addresses associated with the host name.

Click the "Apply" button to save your changes or click the "Clear" button to refresh the page .

4.3 **System Time**

System time can be configured via this page. Administrator can select SNTP Server or from computer to update the system time or administration can use manual setting the system time. Note. If administrator chooses SNTP Server to synchronization update time then must confirm system gateway and DNS is correct and switch system must be able to connect to the SNTP Server.





System Time

- >Source: Select the time source.
 - **SNTP:** Time sync from NTP server.
 - From Computer: Time set from browser host.
 - Manual Time: Time set by manually configure.
- \geq Time Zone: Select a time zone difference from listing district.

SNTP

- Address Type: Select the address type of NTP server. This is enabled when time source is SNTP. \geq
- Server Address: Input IPv4 address or hostname for NTP server. This is enabled when time Source is \geq SNTP.
- \geq IPv6 Address: Input NTP port for NTP server. Default is 123. This is enabled when time source is SNTP. **Manual Time**
- \geq Date: Input manual date. This is enabled when time source is manual.
- \geq Time: Input manual time. This is enabled when time source is manual.

Daylight Saving Time

The Switch support Daylight saving time function, if administrator need enable and set the Daylight saving time function will can be enable this function.





Daylight Saving Ti	me	
Туре	 None Recurring Non-recurring USA Europen 	
Offset	60 Min (1 - 1440, default 60)	
Recurring	From: Day Sun 🗸 Week First 🗸 Month Jan 🗸 Time	
Recurring	To: Day Sun 🗸 Week First 🗸 Month Jan 🗸 Time	
Non-recurring	From: YYYY-MM-DD	HH:MM
Non-recurring	To: YYYY-MM-DD	HH:MM
Operational Status		
Current Time		

```
Apply
```

- \geq **Type:** Select the mode of daylight saving time.
 - **Disable:** Disable daylight saving time.
 - **Recurring:** Using recurring mode of daylight saving time.
 - **Non-Recurring:** Using non-recurring mode of daylight saving time.
 - USA: Using daylight saving time in the United States that starts on the second Sunday of March and ends on the first Sunday of November.
 - **European:** Using daylight saving time in the Europe that starts on the last Sunday in March and ending on the last.
- \geq **Offset :** Specify the adjust offset of daylight saving time.
- **Recurring From:** Specify the starting time of recurring daylight saving time. This field available when \geq selecting "Recurring" mode.
- \geq **Recurring To:** Specify the ending time of recurring daylight saving time. This field available when selecting "Recurring" mode.
- \geq Non-recurring From: Specify the starting time of non-recurring daylight saving time. This field available when selecting "Non-Recurring" mode.
- Non recurring To: Specify the ending time of recurring daylight saving time. This field available when \geq selecting "Non-Recurring" mode.

Operational Status

Current Time: Display the current operating time

Click the "Apply" button to save your changes settings.





5. Port

5.1 **Port setting**

This page shows port current status and allow user to edit port configurations. Select port entry and click "Edit" button to edit port configurations.

Port → Port Setting										
✤ Network	Port	Settin	ig Tabl	e						
– Port										
Port Setting									Q	
Error Disabled S Link Aggregation		Entry	Port	Туре	Description	State	Link Status	Speed	Duplex	Flow Control
EEE		25	GE25	1000M Combo Copper	Managmentport	Enabled	Up	Auto (1000M)	Auto (Full)	Enabled (Off)
Jumbo Frame		27	GE27	1000M Combo Copper		Enabled	Up	Auto (10M)	Auto (Full)	Disabled (Off)
✤ POE Setting		1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
¥ VLAN		2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
✤ MAC Address Table		3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
Spanning Tree		4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
* Discovery		5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
* DHCP		6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
✤ Multicast		7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Field	Description
Port	Display for Port Name.
Туре	Display for Port media type.
Description	Display custom port description.
	Display for Port admin state.
State	• Enabled: Enable the port.
	• Disabled: Disable the port.
	Current port link status.
Link Status	• Up: Port is link up.
	Down: Port is link down.
Speed	Current port speed configuration and link speed status.
Duplex	Current port duplex configuration and link duplex status.
Flow Control	Current port flow control configuration and link flow control status.

Administrator can set speed / Duplex / Flow Control by each port.

Please select port number in checkbox and click apply button to set speed / Duplex / Flow Control of each port.





Port	GE25
Description	Managmentport
State	Z Enable
Speed	 Auto 10M Auto - 10M 100M Auto - 100M 1000M Auto - 1000M
Duplex	 Auto Full Half
Flow Control	 Auto Enable Disable

- **Port:** Selected port list. \geq
- Description: Custom port description
- \geq State: Port admin state.
 - **Enabled:** Enable the port.
 - **Disabled:** Disable the port.
- \geq **Speed:** Port speed capabilities.
 - Auto: Auto speed with all capabilities
 - Auto-10M: Auto speed with 10M ability only
 - Auto-100M: Auto speed with 100M ability only
 - Auto-1000M: Auto speed with 1000M ability only
 - Auto-10M/100M: Auto speed with 10M/100M abilities
 - **10M:** Force speed with 10M ability
 - **100M:** Force speed with 100M ability
 - **1000M:** Force speed with 1000M ability
- \geq **Duplex:** Port duplex capabilities.
 - Auto: Auto duplex with all capabilities
 - Half: Auto speed with 10M and 100M ability only
 - Full: Auto speed with 10M/100M/1000M ability only
- \geq Flow Control: Port flow control.
 - Auto: Auto flow control by negotiation
 - Enabled: Enable flow control ability
 - **Disabled:** Disable flow control ability

Click the "Apply" button to save your changes or "Close" the button to close settings.





5.2 Error Disabled

This function can block of faulty operation, including EPDU Guard / UDLD / Self Loop / Broadcast Flood / Unknown Multicast Flood / Unicast Flood / ACL / Port Security / DHCP Rate Limit / ARP Rate Limit etc. After administrator enable this functions, if occur error in table functions then system will auto immediate block of faulty operation until the after the set time, system will auto re-enable.

Recovery Interval	300	Sec (30 - 86400)
BPDU Guard	Enable	
UDLD	Enable	
Self Loop	Enable	
Broadcast Flood	Enable	
Unknown Multicast Flood	Enable	
Unicast Flood	Enable	
ACL	Enable	
Port Security	Enable	
DHCP Rate Limit	Enable	
ARP Rate Limit	Enable	

Apply

- **Recovery Interval:** Auto recovery after this interval for error disabled port.
- BPDU Guard: Enabled to auto shutdown port when BPDU Guard reason occur.
 *This reason caused by STP BPDU Guard mechanism.
- UDLD: Enabled to auto shutdown port when UDLD violation occur.
- Self Loop: Enabled to auto shutdown port when Self Loop reason occur.
- Broadcast Flood: Enabled to auto shutdown port when Broadcast Flood reason occur.
 *This reason caused by broadcast rate exceed broadcast storm control rate.
- Unknown Multicast Flood: Enabled to auto shutdown port when Unknown Multicast Flood reason occur. This reason caused by unknown multicast rate exceed unknown multicast storm control rate.
- Unicast Flood: Enabled to auto shutdown port when Unicast Flood reason occur. *This reason caused by unicast rate exceed unicast storm control rate.
- ACL: Enabled to auto shutdown port when ACL shutdown port reason occur.
 * This reason caused packet match the ACL shutdown port action.
- Port Security: Enabled to auto shutdown port when Port Security Violation reason occur. *This reason caused by violation port security rules.
- DHCP rate limit: Enabled to auto shutdown port when DHCP rate limit reason occur. *This reason caused by DHCP packet rate exceed DHCP rate limit.
- ARP rate limit: Enabled to auto shutdown port when ARP rate limit reason occur.
 *This reason caused by DHCP packet rate exceed ARP rate limit.

Click the "Apply" button to save your changes settings.





Link Aggregation 5.3

Link Aggregation is also referred to as link aggregation, teaming port, and port trunk for 802.3ad (LACP, Link Aggregation Control Protocol), The Port Aggregation can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

5.3.1 **Group Configuration**

Administrator can select use MAC Address or IP-MAC address of load balance Algorithm. This system default can set 8 LA group, administrator can select LAG number and click Edit button go to set LA used ports.

Port → Link Aggregation	→ Group
– Port	Load Balance Algorithm O MAC Address
Port Setting	
Error Disabled	Apply
Link Aggregation	
Group Port Setting	Link Aggregation Table
LACP	
EEE	
Jumbo Frame	LAG Name Type Link Status Active Member
✤ POE Setting	O LAG 1
¥ VLAN	O LAG 2
MAC Address Table	O LAG 3
 Spanning Tree 	O LAG 4
✤ Discovery	O LAG 5
* DHCP	O LAG 6
✤ Multicast	O LAG 7
 IP Configuration 	0 1403
✤ Security	U LAG 8
* ACL	Edit

 \succ Load Balance Algorithm: LAG load balance distribution algorithm.

- MAC Address: Based on MAC address.
- IP-MAC Address: Based on MAC address and IP address.

Click the "Apply" button to save your changes settings.





Field	Description
LAG	LAG Name.
Name	LAG port description.
Туре	 The type of the LAG. Static: The group of ports assigned to a static LAG are always active members. LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
Link Status	LAG port link status.
Active Member	Active member ports of the LAG.
Inactive Member	Inactive member ports of the LAG.

Edit Link Aggregation Group

LAG	1
Name	LAGGRPOUP-1
Туре	 Static LACP
Member	Available Port Selected Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8
Apply	Close

- LAG: Selected LAG group ID. \geq
- \geq Name: LAG port description.
- **Type:** The type of the LAG.
 - Static: The group of ports assigned to a static LAG are always active members.
 - LACP: The group of ports assigned to dynamic LAG are candidate ports. LACP determines which candidate ports are active member ports.
- \geq Member: Select available port to be LAG group member port.

Click the "Apply" button to save your changes or "Close" the button to close settings.





5.3.2 **Port Setting**

This page shows LAG port current status and allow user to edit LAG port configurations. Select LAG entry and click "Edit" button to edit LAG port configurations.

Status Network	Por	t Settin	g Tab	le					
· Port									Q
Port Setting		LAG	Туре	Description	State	Link Status	Speed	Duplex	Flow Control
Error Disabled		LAG 1		SalesDept	Enabled	Down	Auto	Auto	Enabled
Link Aggregation Group		LAG 2		ACCDept	Enabled	Down	Auto - 100M	Auto	Disabled
Port Setting		LAG 3		ENGDept	Enabled	Down	Auto - 1000M	Auto	Enabled
LACP		LAG 4			Enabled	Down	Auto	Auto	Disabled
EEE		LAG 5			Enabled	Down	Auto	Auto	Disabled
Jumbo Frame		LAG 6			Enabled	Down	Auto	Auto	Disabled
POE Setting		LAG 7			Enabled	Down	Auto	Auto	Disabled
VLAN MAC Address Table		LAG 8	_		Enabled	Down	Auto	Auto	Disabled
Spanning Tree		Edit	1						

Field	Description
LAG	Display for LAG Port Name.
Туре	Display for LAG Port media type.
Description	Display custom LAG Port description.
	LAG Port admin state.
State	• Enabled: Enable the port.
	• Disabled: Disable the port.
	Current LAG port link status.
Link Status	• Up: Port is link up.
	Down: Port is link down.
Speed	Current LAG port speed configuration and link speed status.
Duplex	Current LAG port duplex configuration and link duplex status.
Flow Control	Current LAG port flow control configuration and link flow control status.



Port	LAG2
Description	RDDept
State	Enable
Speed	 Auto 10M Auto - 10M 100M Auto - 100M 1000M Auto - 1000M Auto - 100M
Flow Control	 Auto Enable Disable

- \geq Port: Selected port list.
- \geq **Description:** Custom LAG Port description.
- \geq State: Port admin state.
 - Enabled: Enable the port.
 - **Disabled:** Disable the port.
- \succ Speed: Port speed capabilities.
 - Auto: Auto speed with all capabilities
 - Auto-10M: Auto speed with 10M ability only
 - Auto-100M: Auto speed with 100M ability only
 - Auto-1000M: Auto speed with 1000M ability only
 - Auto-10M/100M: Auto speed with 10M/100M abilities
 - **10M:** Force speed with 10M ability
 - 100M: Force speed with 100M ability
 - **1000M:** Force speed with 1000M ability
- \geq Flow Control: Port flow control.
 - Auto: Auto flow control by negotiation
 - Enabled: Enable flow control ability
 - **Disabled:** Disable flow control ability

Click the "Apply" button to save your changes or "Close" the button to close settings.





5.3.3 LACP

The LACP can aggregate multiple Ethernet ports together to form a logical aggregation group. To upper layer entities, all the physical links in an aggregation group are a single logical link.

Administrator can to configure LACP global and port configurations. Select ports and click "Edit" button to edit port configuration.

Status	*							
Network		Custom	Driority			(1 GEE2E default 20769)		
Port		System	Priority	p2700		(1 - 65535, default 32768)		
Port Setting Error Disabled Link Aggregation Group Port Setting		pply P Port) t Settii	ng Table				
Fort Setting								
LACP								0
LACP EEE								C
		Entry	Port	Port Priority	Timeout			C
EEE		Entry 1	Port GE1	Port Priority	Timeout Short		_	C
EEE Jumbo Frame				Port Priority 1 2			_	C
EEE Jumbo Frame POE Setting VLAN		1	GE1	1	Short		-	C
EEE Jumbo Frame POE Setting VLAN MAC Address Table		1 2 3	GE1 GE2 GE3	1 2	Short Long Short			C
EEE Jumbo Frame POE Setting VLAN MAC Address Table Spanning Tree		1 2 3 4	GE1 GE2 GE3 GE4	1 2 5	Short Long Short Short			C
EEE Jumbo Frame POE Setting		1 2 3	GE1 GE2 GE3	1 2 5	Short Long Short			(

System Priority: Administrator configures the LACP system priority on each switch running LACP. LACP uses the system priority with the switch MAC address to form the system ID and also during negotiation with other switches. This decides the system priority field in LACP PDU.

Click the "Apply" button to save your changes settings.

The function with the lower system priority value determines which links between LACP partner devices are active and which are in standby for each LACP group. The device on the controlling end of the link uses port priorities to determine which ports are bundled into the aggregated bundle and which ports are put in standby mode. Port priorities on the other device (the no controlling end of the link) are ignored. In priority comparisons, Note numerically lower values have higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the device MAC address determines which switch is in control.





Field	Description
Port	Port Name.
Port Priority	LACP priority value of the port.
	The periodic transmissions type of LACP PDUs.
Timeout	 Long: Transmit LACP PDU with slow periodic (30s).
	 Short: Transmit LACPP DU with fast periodic (1s).

it LACP Port Se	etting	
Port	GE1	
Port Priority	1	(1 - 65535, default 1)
Timeout	 Long Short 	
Apply	Close	

- Port: Selected port list. \geq
- **Port Priority:** Enter the LACP priority value of the port. \geq
- \geq **Timeout:** The periodic transmissions type of LACP PDUs.
 - Long: Transmit LACP PDU with slow periodic (30s).
 - **Short:** Transmit LACPP DU with fast periodic (1s).

5.4 EEE

Energy Efficient Ethernet (EEE) combines the MAC with a family of physical layers that support operation in a low power mode. It is defined by IEEE 802.3az Energy Efficient Task Force. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

This switch support Energy-effcient Ethernet(EEE) function. Administrator can by ports to setting Enable or Disable for the EEE function. The default is "Disable".



USER MANUAL

Port → EEE					
≽ Status	^				
✓ Network	EE	E Settir	ng Tab	le	
– Port					
Port Setting					Q,
Error Disabled		Entry	Port	State	
Link Aggregation		1	GE1	Enabled	
Group					
Port Setting		2	GE2	Enabled	
LACP		3	GE3	Enabled	
EEE		4	GE4	Enabled	
Jumbo Frame		5	GE5	Enabled	
POE Setting					
VLAN		6	GE6	Disabled	
MAC Address Table		7	GE7	Enabled	
1990 8040 00-00		8	GE8	Disabled	
		9	GE9	Enabled	
Solution Discovery		v	OLU	Enabled	

Field	Description
Port	Port Name
State/Operational Status	 Port EEE admin state. Enabled: EEE is enabled/ is operating Disabled: EEE is disabled/ is no operating

Edit EEE Se	etting
_	
	GE3,GE7,GE9,GE12-GE13
State	C Enable
Apply	Close

- \succ Port: Selected port list.
- \geq **State:** Port EEE admin state.
 - Enable: Enable EEE
 - **Disable:** Disable EEE

Click the "Apply" button to save your changes or "Close" the button to close settings.

+(886) 2-8911-6160





Jumbo Frame 5.5

The administrator can set the Jumbo Frame size and display it on this page.

Port 🖶 Jumbo Frame			
* Network		Z Enable	
 Port Port Setting Error Disabled ink Aggregation Group Port Setting LACP EEE 	Jumbo Frame	10000	Byte (1518 - 10000, default 1522)
Jumbo Frame			

 \geq Jumbo Frame: Enable or disable jumbo frame. When jumbo frame is enabled, switch max frame size is allowed to configure. When jumbo frame is disabled, default frame size 1522 will be used.

allowed to be configured. Note Uncheck to apply : When you click uncheck to "Apply", The switch will back to default regular frame size "1522".

Click the "Apply" button to save your changes settings.

6. POE

PoE or Power over Ethernet is an IEEE standard used to pass electrical power along with data over standard Ethernet Cable. Utilising 2 of the 4 pairs of an Ethernet Cable PoE provides up to 15.4W (IEEE 802.3af) or 25.5W (IEEE 802.3at) of power. PoE is used to power devices such as IP Cameras, Wireless Access Points and IP Phone. Being able to use a single cable to run both data and power saves in cabling costs, helps unclutter messy cables on your desk and is perfect for those environments where a power point is not able to be installed where your Ethernet equipment is needed. The PoE switches are IEEE 802.3at compliant and can supply up to 25.5W per port. Advanced features such as PoE Power scheduling, PoE priority and having the ability to allocate a particular amount of power per port are just some of the features that the PoE Switch support.

6.1 **POE Port Setting**

This page system can displayed PoE port is enable or disable and on /off , calculate used PoE type /PoE Level / Actual power(mW) / Power Voltage(V) / Current(mA), Refresh Rate None or 5/10/30sec information.



USER MANUAL

×

×

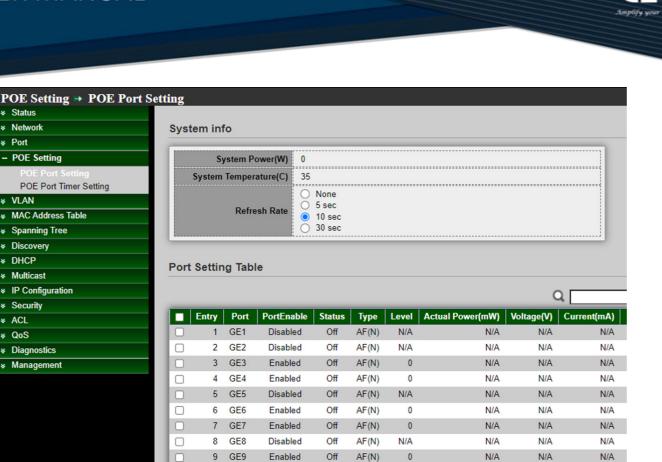
×

×

×

×

×



System Power(W) : Display the POE system power (Watt).

10 **GE10** Enabled

- **System Temperature(C) :** Display the system temperature (°C). >
- \triangleright Refresh Rate : Refresh the web page every period of "None, 5 sec, 10 sec, 30 sec "seconds base to get new counter of specified POE port.

Off

AF(N)

0

N/A

N/A

N/A

Field	Description
Port	Port Name.
Port Enable	 Port admin state. Enabled: POE Port is enabled. Disabled: POE Port is disabled.
Status	 Port POE admin state. On: POE is operating. Off: POE is no operating.
Туре	Display the type of POE, including AF (Y) connected / AF (N) not connected / AT (Y) connected / AT (N) not connected.
Level	Display the Class level used by POE, displayed 0/1/2/3/4 as Class0 / Class1 / Class2 /Class3 / Class4.
Actual Power(mW)	Display the POE actual power used (mW).





Voltage(V)	Display the POE Voltage used (V).
Current(mA)	Display the POE Current used (mA).
Select the port Edit Port Setting	form 1 - 24 port to be set, and click "Edit" to edit the settings.
Port	GE1,GE3,GE7-GE8
PortEnable	 Enable Disable
Apply	Close

This section is used to enable/disable PoE on a per port basis, set the POE enable/disable per port on this PoE switches.

- **Port :** Will be displayed based on your selection.
 - Enable : PoE enabled for the port.
 - **Disable :** PoE disabled for the port.

Click the "Apply" button to save your changes or "Close" the button to close settings.

6.2 POE Port Time Setting

The PoE switch supports a PoE scheduling feature that allows administrators to turn off devices when they are not in use. This can be used as a power saving function, or as a power restart control for the PD device. At the same time, the power consumption of the switch can be effectively limited through the power time control. To configure the PoE Scheduling function via the Web Interface, Set the desired time for the device to power on by ticking and checkbox and modify for your configuration.

POE Setting POE Port T	'imer Setti	ing								
✤ Status		-								
✤ Network	Port	GE1 V								
∗ Port	L	GE1 GE2								
POE Setting		GE3		_			_	_	_	_
∗ VLAN		GE4	03	04	05	06	07	08	09	10
MAC Address Table	Mon	GE5 GE6								
✤ Spanning Tree	Tue	GE7		✓	✓	✓	✓	✓	✓	✓
* Discovery	Wed	GE8								
* DHCP	Thu	GE9 GE10			 Image: A start of the start of	✓	✓	✓	✓	✓
≽ Multicast	Fri	GE11	2							
✤ IP Configuration	Sat	GE12 GE13	2		 Image: A second s	 Image: A start of the start of		 Image: A start of the start of	 Image: A start of the start of	Image: A start of the start



 \geq **Port :** Select one port to set time schedule.

<	00	01	02	03	04	05	06	07	08	09	10	11	12	13
Wed	 Image: A start of the start of	~	Image: A start of the start	~	~		~			 Image: A start of the start of	~	 Image: A start of the start of		 Image: A start of the start of
Tue	 Image: A start of the start of	✓	 Image: A start of the start of	 Image: A start of the start of					 Image: A start of the start of	 Image: A start of the start of	 Image: A start of the start of	 Image: A second s	 Image: A start of the start of	 Image: A start of the start of
Thu														
Sun										✓		✓		✓
Sat				Z						~				
Mon	 Image: A start of the start of	 Image: A start of the start of					 Image: A start of the start of	 Image: A start of the start of		✓	 Image: A start of the start of	<	 Image: A set of the set of the	 Image: A start of the start of
Fri														

 \geq Mon/Tue/Wed/Thu/Fri/Sat/Sun : Select POE start time based on Monday-Sunday and 00-23 hours.

Click the "Apply" button to save your changes settings.

7. VLAN

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together even if they are not located on the same network switch.

The CS-2424G-24P A5 adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

Administrator can set IEEE 802.1q Tag Based VLAN or Port Based VLAN. System default is VLAN1 Port based (PVID).

7.1 VLAN

7.1.1 **Create VLAN**

Administrator can select VLAN number in Available VLAN list, this VLAN number based on IEEE 802.1q standard. Available VLAN list can be multiple choices.





VLAN 🔿 VLAN 🗭 Create VLAN			
Status			
* Network	Available VLAN	Created	VLAN
♥ Port	VLAN 2	VLAN 1	
POE Setting		VLAN 1	094
- VLAN		>	
⊗ VLAN	VLAN 5		
Create VLAN	VLAN 6 VLAN 7	<	
VLAN Configuration	VLAN 8		
Membership	VLAN 9 🚽		-
Port Setting	E		
S Voice VLAN			
Protocol VLAN Apply			
MAC VLAN VLAN Tal	ماه		
Surveillance VLAN	516		
© GVRP Showing All	✓ entries		Showing 1
✓ MAC Address Table			Ű
Spanning Tree	AN Name	Туре	VLAN Interface State
✤ Discovery	default	Default	Enabled
* DHCP 24094	4 VLAN4094	Static	Disabled
♥ Multicast			
* IP Configuration Edit	Delete		

> VLAN: Administrator can select VLANs number in "Available VLAN" table and move to "Created VLAN" table will complete the 802.1q VLAN.

Click the "Apply" button to save your changes settings.

VLAN Table: Administrator can checkbox VLAN to edit or delete, if check and click "Edit" button then administrator can manual modify name description for this VLAN.

Edit VLAN I	
Name	VLAN4094
Apply	Close

Click the "Apply" button to save your changes or "Close" the button to close settings.

7.1.2 **VLAN Configuration**

Administrator can choose set Excluded / Forbidden / Tagged / Untagged function in membership table of the Port and LAG.





VLAN > VLAN > VLA	N Configur	ation										
≽ Status	^											
➢ Network	VLAN	VLAN Configuration Table										
≽ Port												
✤ POE Setting	VLAN	VLAN VLAN4094 V										
- VLAN												
⊗ VLAN	Entry	Port	Mode		Membership)	PVID	Forbidde				
Create VLAN	1	GE1	Trunk	Excluded	O Tagged	Untagged						
VLAN Configuration	2	GE2	Trunk	CExcluded	◯ Tagged	Untagged						
Membership Port Setting	3	GE3	Trunk	Excluded	○ Tagged	◯ Untagged						
 Voice VLAN 	4	GE4	Trunk	Excluded	◯ Tagged	O Untagged						
Protocol VLAN	5	GE5	Trunk	CExcluded	Tagged	O Untagged						
S MAC VLAN	6	GE6	Trunk	CExcluded	Tagged	O Untagged						
 Surveillance VLAN GVRP 	7	GE7	Trunk	Excluded	O Tagged	O Untagged		~				
MAC Address Table	8	GE8	Trunk	Excluded	◯ Tagged	O Untagged						
Spanning Tree	9	GE9	Trunk	Excluded	O Tagged	O Untagged		~				
 Discovery 	10	GE10	Trunk	Excluded	○ Tagged	O Untagged						
* DHCP	11	GE11	Trunk	Excluded	○ Tagged	○ Untagged						
					0	0						

Field	Description				
VLAN	Select specified VLAN ID to configure VLAN configuration.				
Port	Display the interface of port entry.				
Mode	Display the interface VLAN mode of port.				
Membership	 Select the membership for this port of the specified VLAN ID. Forbidden: Specify the port is forbidden in the VLAN. Excluded: Specify the port is excluded in the VLAN. Tagged: Specify the port is tagged member in the VLAN. Untagged: Specify the port is untagged member in the VLAN. 				
PVID	Display if it is PVID of interface.				
Forbidden	Forbidden: Specify the port is forbidden in the VLAN.				

 \geq VLAN: Administrator can click drop down menu to choose VLAN and set.

- **Excluded:** This interface is currently not a member of the VLAN. This is the default for all the ports and LAGs.
- Tagged: This interface is a tagged member of the VLAN.
- Untagged: This interface is an untagged member of the VLAN. Frames of the VLAN are sent untagged to the interface VLAN.
- **PVID**: Check to set the PVID of the interface to the VID of the VLAN. PVID is a per-port setting.
- Forbidden: Select for this specified port of the Forbidden.





7.1.3 Membership

Display all port setting information. Administrator can checkbox and click "Edit" button to modify VLAN type. (Note: Number=VLAN number, F=Forbidden, T=Tagged, U=Untagged, P=PVID)

When a port is forbidden default VLAN membership, that port is not allowed membership in any other VLAN. An internal VID of 4095 is assigned to the port. This PVID on the ports between the two devices must be the same if the ports are to send and receive untagged packets to and from the VLAN. Otherwise, traffic might leak from one VLAN to another.

VLAN → VLAN → Members	hip						
♦ Network	Mem	nbersh	ip Tab	le			
✤ Port							
✤ POE Setting							Q,
- VLAN		Entry	Port	Mode	Administrative VLAN	Operational VLAN	
⊗ VLAN	0	1	GE1	Trunk	1UP	1UP	
Create VLAN VLAN Configuration	0	2	GE2	Trunk	1UP	1UP	
Membership	0	3	GE3	Trunk	1UP	1UP	
Port Setting	0	4	GE4	Trunk	1UP	1UP	
S Voice VLAN	0	5	GE5	Trunk	1UP	1UP	
 Protocol VLAN MAC VLAN 	0	6	GE6	Trunk	1UP	1UP	
Surveillance VLAN	0	7	GE7	Trunk	1UP	1UP	
© GVRP	0	8	GE8	Trunk	1UP	1UP	
MAC Address Table	0	9	GE9	Trunk	1UP	1UP	
 Spanning Tree 	0	10	GE10	Trunk	1UP	1UP	

Field	Description
Port	Display the interface of port entry.
Mode	Display the interface VLAN mode of port.
Administrative VLAN	Display the administrative VLAN list of this port.
Operational VLAN	Display the operational VLAN list of this port. Operational VLAN means the VLAN status that really runs in device. It may different to administrative VLAN.







Edit Port Setting	
Port	GE3
Mode	Trunk
Membership	4094 1UP IUP IUP IVP IVP IVP IVP IVP IVP IVP IV
Apply	Close

- \succ **Port:** Display selected port number.
- **Mode:** Displays the port VLAN mode that was selected on the Interface Settings page. \geq
- \geq Membership: Move the VLAN IDs from the left list to the right list by using the arrow buttons. The default VLAN might appear in the right list if it is tagged, but it cannot be selected.

7.1.4 **Port Setting**

Administrator can set Access / Trunk / Hybrid for VLAN mode.

VLAN >> VLAN >> Port	Setting								
≽ Status	^								
	Port	Settin	ng Tabl	le					
∗ Port									
✤ POE Setting							Q		
- VLAN		Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
⊗ VLAN		1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
Create VLAN VLAN Configuration		2	GE2	Trunk	1	All	Enabled	Disabled	0x8100
Membership		3	GE3	Hybrid	4094	Untag Only	Enabled	Disabled	0x8100
Port Setting			GE4	Hybrid		Tag Only	Disabled	Disabled	0x8100
S Voice VLAN			GE5	Hybrid		Tag Only	Disabled	Disabled	0x8100
 Protocol VLAN MAC VLAN 		6	GE6	Hybrid	1	Tag Only	Disabled	Disabled	0x8100
 MAC VLAN Surveillance VLAN 		7	GE7	Hybrid	1	Tag Only	Disabled	Disabled	0x8100
© GVRP		8	GE8	Hybrid	1	Tag Only	Disabled	Disabled	0x8100
MAC Address Table		9	GE9	Hybrid	1	Tag Only	Disabled	Disabled	0x8100
Spanning Tree		10	GE10	Hybrid	1	Tag Only	Disabled	Disabled	0x8100





Field	Description
Port	Display the interface.
Mode	Display the VLAN mode for Hybrid/Access/Trunk/Tunnel mode of port.
PVID	Display the Port-based VLAN ID of port.
Accept Frame Type	Display accept frame type of port.
Ingress Filtering	Display ingress filter status of port.
Uplink	Display uplink status.
TPID	Display TPID used of interface.

Port	GE4-GE10
Mode	 Hybrid Access Trunk Tunnel
PVID	1 (1 - 4094)
Accept Frame Type	 All Tag Only Untag Only
Ingress Filtering	🗌 Enable
Uplink	Enable
TPID	0x8100 🗸

- \geq **Hybrid:** The interface can be a tagged or untagged member of one or more VLANs.
- > Access: The interface is an untagged member of a single VLAN. A port configured in this mode is known as an access port.
- \geq Trunk: The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs. A port configured in this mode is known as a trunk port.
- \geq **Tunnel:** This enables the user to use own VLAN arrangements (PVID) across the provider network.
- \geq **PVID:** Enter the Port VLAN ID (PVID) of the VLAN to which incoming untagged and priority tagged frames are classified.
- \geq Accept Frame Type: Select the type of frame that the interface can receive. Frames that are not of the configured frame type are discarded at ingress. These frame types are only available in General mode. As follow.





- All: The interface accepts all types of frames: untagged frames, tagged frames, and priority tagged frames.
- **Tag Only:** The interface accepts only tagged frames.
- Untag Only: The interface accepts only untagged and priority frames.
- \geq Ingress Filtering: Administrator can check Enable to enable ingress filtering. When an interface is ingress filtering enabled, the interface discards all incoming frames that are classified as VLANs of which the interface is not a member. Ingress filtering can be disabled or enabled on general ports. It is always enabled on access ports and trunk ports.
- \geq **Uplink:** Administrator can check **Enable** to set the interface as an uplink port.
- \geq **TPID:** If Unlink is enabled, select the Modified Tag Protocol Identifier (TPID) value for the interface.

Voice VLAN 7.2

Voice VLAN allows you to enhance VoIP service by configuring ports to carry IP Voice traffic from IP phones on a specific VLAN. VoIP traffic has a preconfigured OUI prefix in the source MAC address. Administrator can set VLAN ID in the range of 1 to 4094.

7.2.1 Property

VLAN → Voice VLAN → Pro	perty						
		S	itate	Enable			
✤ Port							
✤ POE Setting		V	LAN	VLAN4094	~		
- VLAN	C	oS / 80	2 1 n	Enable			
⊗ VLAN		Remar		5 🗸			
Create VLAN		Aging 1	Time	1440	Mi	n (30 - 65536, d	efault 1440)
VLAN Configuration		- Alua					
Membership	(1				
Port Setting	Ap	ply	ļ				
Property	-						
Voice OUI	Port S	Settin	g lab	le			
Protocol VLAN							
MAC VLAN							Q. [
Surveillance VLAN		_	-				
S GVRP		Entry	Port	State	Mode	QoS Policy	
* MAC Address Table		1	GE1	Disabled	Auto	Voice Packet	
✤ Spanning Tree		2	GE2	Disabled	Auto	Voice Packet	
* Discovery		3	GE3	Disabled	Auto	Voice Packet	
* DHCP		4	GE4	Disabled	Auto	Voice Packet	
* Multicast		5	GE5	Disabled	Auto	Voice Packet	

Click the "Apply" button to save your changes settings.



USER MANUAL



Field	Description
Port	Display port entry.
State	Display enable/disabled status of interface.
Mode	Display voice VLAN mode.
QoS Policy	Display voice VLAN remark will effect which kind of packet.

Edit Port Setting Port	GE1
State	Enable
Mode	 Auto Manual
QoS Policy	Voice Packet All
Apply	Close

- State: Administrator can choose Enable or Disable this function.
- > VLAN: Administrator can choose VLAN.
- **Cos / 802.1P Remarking**: Administrator can set CoS 802.1p priority level for the VLAN.
- > **Port Aging Time:** Administrator can set aging time for this rule.

Click the "Apply" button to save your changes or "Close" the button to close settings.

7.2.2 Voice OUI

Organizationally Unique Identifiers (OUI) is the first three bytes of a MAC Address, while the last three bytes contain a unique station ID. Administrator can add a specific manufacturer with the OUI. Once the OUI is added, all traffic received on voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN. Unlike the telephony OUI mode that detects voice devices based on telephony OUI, Auto Voice VLAN mode depends on auto smart port to dynamically add the ports to the voice VLAN. The default has set 8 companies for the voice phone.





VLAN → Voice VLAN →	Voice OUI		
* Network	Voice O	UI Table	
≽ Port			
✤ POE Setting	Showing A	All 🗸 entries	
- VLAN		OUI	Description
 VLAN Create VLAN 	✓	00:E0:BB	3COM
VLAN Configuration		00:03:6B	Cisco
Membership		00:E0:75	Veritel
Port Setting		00:D0:1E	Pingtel
		00:01:E3	Siemens
Property Voice OUI		00:60:B9	NEC/Philips
Protocol VLAN		00:0F:E2	H3C
MAC VLAN		00:09:6E	Avaya
 Surveillance VLAN GVRP 	Add	Edit	Delete

Field	Description
OUI	Display OUI MAC address.
Description	Display description of OUI entry.

Edit Voice OUI	
OUI	00:03:6B
Description	Cisco
Apply	Close

Administrator can create new OUI or modify or delete OUI in table

Click "add" button can create new OUI.

Click "Edit" button can modify OUI data.

Click "Delete" button can delete OUI data.

Click the *"Apply"* button to save your changes or *"Close"* the button to close settings.

+(886) 2-8911-6160





Protocol VLAN 7.3

7.3.1 **Protocol Group**

Administrator can configure this page to add or edit groups settings of protocol VLAN, Setting "add" and "Edit" and "Delete" function for this management.

VLAN -> Protocol VLAN -> Protocol Group			
	Protocol Group	Table	
✤ Port			
✤ POE Setting	Showing All 🗸 entri	es	Showing 1 to 2 of 2 entries
– VLAN	Group ID	Frame Type	Protocol Value
 VLAN Create VLAN VLAN Configuration Membership Port Setting Voice VLAN Property Voice OUI Protocol VLAN 	1 RF 2 IEI	C_1042 EE802.3_LLC_Other Edit Delete	0x0600 0x0601
Protocol Group Group Binding MAC VLAN Surveillance VLAN GVRP			

Field	Description
Group ID	Display group ID of entry.
Frame Type	Display frame type of entry.
Protocol Value	Display protocol value of entry.

Add Protocol Group			
Group ID	1 •		
Frame Type	Ethernet_II	 Image: A set of the set of the	
Protocol Value	Ethernet_II IEEE802.3_LLC_Other RFC_1042	(0:	x600 ~ 0xFFFE)
Apply Clo	se		

- **Group ID :** Select group ID of list. The range from 1 to 8. \geq
- Frame Type : Select frame type of list that maps packets to protocol-defined VLANs by examining \geq the type octet within the packet header to discover the type of protocol associated with it.
 - **Ethernet_II** : packet type is Ethernet version 2.





- IEEE802.3_LLC_Other : packet type is 802.3 packet with LLC other header.
- **RFC_1042** : packet type is rfc 1042 packet.
- \succ Protocol Value : Input protocol value of the target protocol. Packets match this protocol value classified to specified VLAN ID.

7.3.2 **Group Binding**

Administrator can configure this bind protocol VLAN group to each port with VLAN ID, Setting "add" and "Edit" and "Delete" function for this management.

✓ Network	Group Binding Table	
≱ Port		
FOR Setting	Showing All 🗸 entries	Showing 1 to 2 of 2 entries
- VLAN	Port Group ID VLAN	
VLAN Create VLAN	GE5 2 4094	
VLAN Configuration	GE6 2 4094	
Membership	Add Edit De	elete
Port Setting		
Voice VLAN Property		
Voice OUI		
Protocol Group		
Group Binding		

Field	Description
Port	Display port ID that binding with protocol group entry.
Group ID	Display group ID that port binding with.
VLAN	Display VLAN ID that assign to packets which match protocol group.



Port	Available Port	
Group ID	2 🗸	
VLAN	4094 (1 -	4094)

- \geq **Port :** Select ports in left box then move to right to binding with protocol group. Or select ports in right box then move to left to unbind with protocol group. Only interface has hybrid VLAN mode can be selected and bound with protocol group. Only available on Add dialog.
- \geq Group ID : Select a Group ID to associate with port. Only available on Add dialog.
- \geq **VLAN** : Input VLAN ID that will assign to packets which match protocol group.

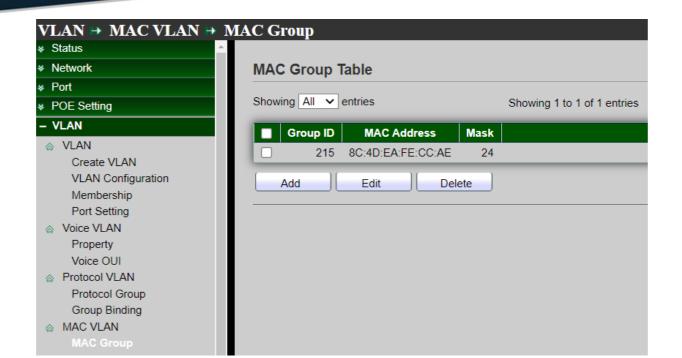
MAC VLAN 7.4

7.4.1 **MAC Group**

The MAC VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet. You define a MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified using a source MAC address and the appropriate VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (i.e., there is a system-wide table that has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged it will maintain this value; otherwise, the priority will be set to 0 (zero). The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid, ingress processing on the packet continues; otherwise, the packet is dropped. This implies that you can configure a MAC address mapping to a VLAN that has not been created on the system, Setting "add" and "Edit" and "Delete" function for this management.





Field	Description
Group ID	Display group ID of entry.
MAC Address	Display mac address of entry.
Mask	Display mask of mac address for classified packet.

			-	-		
<u>^</u>		MAA	C	C	0	un
Au	u	IVIA		G	0	up

Group ID	215	(1 - 2147483647)
MAC Address	8C:4D:EA:FE:CC:AE	(A:B:C:D:E:F)
Mask	24	(9 - 48)
Apply C	lose	

- \geq Group ID: Add a Group ID number.
- MAC Address : Enter the MAC Address. \geq
- \triangleright Mask: Enter the mask of mac address for classified packet..





Group Binding 7.4.2

The Group Binding allows user to bind MAC VLAN group to each port with VLAN ID, Setting "add" and "Edit" and "Delete" function for this management.

VLAN → MAC VLAN → Gr	oup Binding
♦ Network	Group Binding Table
¥ Port	
	Showing All v entries Showing 1 to 1 of 1 entries Q
– VLAN	Port Group ID VLAN
⊗ VLAN	GE8 215 4094
Create VLAN	
VLAN Configuration	First Previous
Membership	Add Edit Delete
Port Setting	
Property	
Voice OUI	
Protocol Group	
Group Binding	
MAC Group	
Group Binding	

Field	Description				
Field	Description.				
Port	Display port ID that binding with protocol group entry.				
Group ID	Display group ID that port binding with.				
VLAN	Display VLAN ID that assign to packets which match protocol group.				



Add Group Bin	Available Port Selected Port GE3 GE4 GE5 GE6 GE7 GE9 GE10 VLAN Hybrid port can be set MAC VLAN
Group ID	215 🗸
VLAN	4094 (1 - 4094)
Apply	Close

- Port: Select the port in the left frame and move to the right to bind to the mac group; or select the port in the right frame and move to the left to bind to the mac group. Only interfaces with mixed VLAN mode can be selected and bound to the protocol group.
- **Group ID:** Choose a Group ID associated with the port. \geq
- \geq **VLAN**: Enter the VLAN ID that will be assigned to packets matching the MAC Group.

Surveillance VLAN 7.5

7.5.1 **Property**

Administrator can configure this page to configure global and per interface settings of Surveillance VLAN.





Status						
Network		State	Enable			
Port		VLAN				
POE Setting		VLAN	VLAN4094	•		
VLAN	Co	S / 802.1p	Enable			
VLAN	R	emarking	6 🗸			
Create VLAN	Ac	ging Time	1440	Mi	n (30 - 65536,	default 144
VLAN Configuration Membership			L			
Port Setting Voice VLAN	Apply	y				
 Voice VLAN Property Voice OUI 		etting Tal	ble			
Voice VLAN Property	Port Se	etting Tal		Mada		٩
Voice VLAN Property Voice OUI Protocol VLAN Protocol Group Group Binding MAC VLAN	Port Se	etting Tal	State	Mode	QoS Policy	٩
Voice VLAN Property Voice OUI Protocol VLAN Protocol Group Group Binding MAC VLAN MAC Group	Port Se	etting Tal		Mode Auto	QoS Policy Video Packet	Q
Voice VLAN Property Voice OUI Protocol VLAN Protocol Group Group Binding MAC VLAN MAC Group Group Binding	Port Se	etting Tal	State			
Voice VLAN Property Voice OUI Protocol VLAN Protocol Group Group Binding MAC VLAN MAC Group	Port Se	etting Tal	State Disabled	Auto	Video Packet	t

- \geq State : Set checkbox to enable or disable Surveillance VLAN function.
- VLAN : Select Surveillance VLAN ID. Surveillance VLAN ID cannot be default VLAN. \geq
- \geq **Cos/802.1p** : Select a value of VPT. Qualified packets will use this VPT value as inner priority.
- \geq **Remarking:** Set checkbox to enable or disable 1p remarking. If enabled, qualified packets will be remark by this value.
- \geq Aging Time : Input value of aging time. Default is 1440 minutes. A video VLAN entry will be age out after this time if without any packet pass through.

Click the "Apply" button to save your changes settings.

Port	Port Setting Table										
							C	2			
	Entry	Port	State	Mode	QoS Policy						
	1	GE1	Disabled	Auto	Video Packet						
	2	GE2	Disabled	Auto	Video Packet						
	3	GE3	Disabled	Auto	Video Packet						
	4	GE4	Disabled	Auto	Video Packet						
	5	GE5	Disabled	Auto	Video Packet						
	6	GE6	Disabled	Auto	Video Packet						
	7	GE7	Disabled	Auto	Video Packet						
	8	GE8	Disabled	Auto	Video Packet						
	9	GE9	Disabled	Auto	Video Packet						
	10	GE10	Disabled	Auto	Video Packet						
	11	GE11	Disabled	Auto	Video Packet						
	12	GE12	Disabled	Auto	Video Packet						





Field	Description					
Port	Display port entry.					
State	Display enable/disabled status of interface.					
Mode	Display voice VLAN mode.					
QoS Policy	Display Surveillance VLAN remark will effect which kind of packet.					

Edit Port Setting	1
Port	GE2-GE4
State	Enable
Mode	● Auto ○ Manual
QoS Policy	 Video Packet All
Apply	Close

- \geq **Port :** Display selected port to be edited.
- **State** : Set checkbox to enable/disabled Surveillance VLAN function of interface. \geq
- \geq Mode : Select port Surveillance VLAN mode.

Auto : Video VLAN auto detect packets that match OUI table and add received port into surveillance VLAN ID tagged member.

- Manual : User need add interface to VLAN ID tagged member manually.
- **QoS Policy :** Select port QoS Policy mode.

Video Packet : Video Packet: QoS attributes are applied to packets with OUIs in the source MAC address.

All : QoS attributes are applied to packets that are classified to the Surveillance VLAN.

Click the "Apply" button to save your changes or "Close" the button to close settings.

7.5.2 Surveillance OUI

Administrator can configure this page to add, edit or delete OUI MAC addresses, Setting "add" and "Edit" and "Delete" function for this management.

 \geq





VLAN Surveillance VLAN	N → Surveillance OUI
★ Status ▲	
✤ Network	Surveillance OUI Table
✤ Port	
✤ POE Setting	Showing All v entries Showing 1 to 1 of 1 entries Q
– VLAN	OUI Description
⊗ VLAN	84:40:EA CAM1
Create VLAN	
VLAN Configuration	First Previous 1
Membership	Add Edit Delete
Port Setting	
Property	
Voice OUI	
Protocol Group	
Group Binding	
MAC Group	
Group Binding	
Surveillance VLAN	
Property	
Surveillance OUI	

Field	Description						
OUI	Display OUI MAC address.						
	Display description of OUI entry.						
Description	Display description of OUI entry.						
	Display description of OUI entry.						
Description Add Surveillance OUI OUI 84	Display description of OUI entry.						

- OUI : Input OUI MAC address. Can't be edited in edit dialog. \geq
- \geq **Description :** Input description of the specified MAC address to the Surveillance VLAN OUI table.

7.6 **GVRP**

The GVRP (Generic VLAN Registration Protocol) is described in the IEEE 802.1p standard; It's an IEEE 802.1Q-compliant method for facilitating automatic (dynamic) VLAN membership configuration. GVRP-enabled switches can exchange VLAN configuration information with other GVRP-enabled switches.







Policy rules or other network management methods can determine who is admitted to a VLAN. When a node requests admission to a specific VLAN, GVRP handles the registration of the node with GVRP-enabled switches and maintains that information.

GVRP reduces the chance of errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. In addition, you can use GVRP to dynamically enable port membership in static VLANs configured on a switch. Once GVRP creates a dynamic VLAN will can also reduce unnecessary broadcast traffic and unicast traffic.

7.6.1 Property

Administrator can enable GVRP function and set every port registration on GVRP.

VLAN 🖶 GVKP 🖶 Property	y						
∗ Status <u>^</u>							
* Network		State		Enable			
¥ Port	1.000						
POE Setting	Ope	erationa	I Time	out			
– VLAN		Join	20		cs	; (2 - 16375, defaul	t 20)
⊗ VLAN							,
Create VLAN		Leave	60		CS	s (45 - 32760, defau	ılt 60)
VLAN Configuration		eaveAll	100	0		s (65 - 32765, defau	ut 1000)
Membership Port Setting		eaveAn			CS		
 ➢ Voice VLAN Property Voice OUI ➢ Protocol VLAN Protocol Group 		oply Setting	g Tabl	e			
Group Binding							Q
MAC VLAN MAC Group		Entry	Port	State	VLAN Creation	n Registration	
Group Binding		1	GE1	Disabled	Enabled	Normal	
		2	GE2	Disabled	Enabled	Fixed	
Property		3	GE3	Disabled	Enabled	Fixed	
Surveillance OUI		4	GE4	Disabled	Enabled	Fixed	
⊗ GVRP Property		5	GE5	Disabled	Enabled	Normal	

- \geq State : Set the enabling status of GVRP functionality
 - Enable: if Checked Enable GVRP, else is Disable GVRP.
- \geq Operational Timeout: The port will not learn any dynamic VLAN. Only send static VLAN information to
 - Join.: GVRP Join time out.
 - Leave: GVRP leave time out.

Click the "Apply" button to save your changes settings.

Field	Description
Port	Port Name.
State	Display port GVRP state.





VLAN Creation	Display port GVRP creation VLAN state.
Registration	Display port GVRP registration mode.

E	d	it	P	0	r	S	e	tt	i	n	g	J		
						 	-		-	-			-	

State Enable VLAN Creation Image: Enable Registration Normal Fixed Forbidden	Port	GE2-GE4
O Normal Registration Sized	State	Enable
Registration 🔘 Fixed	VLAN Creation	Enable
	Registration	Fixed

- Port: Display port number. \succ
- \geq **State:** Displays whether GVRP is enabled or disabled on the interface.
- VLAN Creation: Displays whether Dynamic VLAN creation is enabled or disabled on the interface. \geq If it is disabled, GVRP can operate but new VLANs are not created.
- \geq **Registration:** Displays the VLAN registration mode on the interface.
 - Normal: Normal mode..

Fixed: The port will not learn any dynamic VLAN. Only send static VLAN information to neighbor and allow static VLAN packet pass..

Forbidden: The port will not learn any dynamic VLAN and only allow default VLAN packet pass.

Click the "Apply" button to save your changes or "Close" the button to close settings.

7.6.2 **Member ship**

When enable GVRP function and state ports in GVRP then administrator can check GVRP member information.



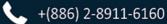


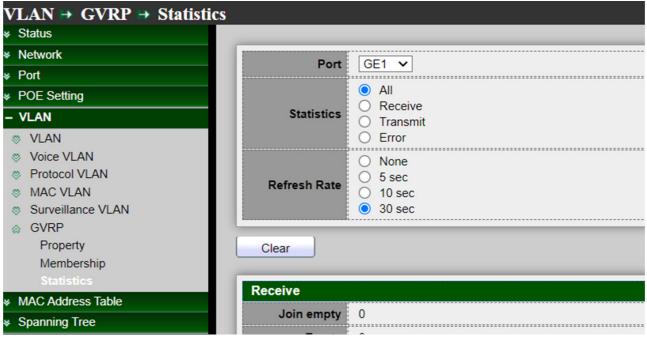
VLAN → GVRP → Mem	ibership
	Membership Table
≉ Port	
✤ POE Setting	Showing All entries Showing 0 to 0 of 0 entries
– VLAN	VLAN Member Dynamic Member Type
♥ VLAN	0 results found.
Voice VLAN	
Protocol VLAN	First Previous
MAC VLAN	
Surveillance VLAN	
⊗ GVRP	
Property	
Statistics	

Field	eld Description	
VLAN ID.		
Member VLAN port members include static and dynamic member.		
Dynamic Ports GVRP learned dynamic ports.		
Туре	The type of VLAN is static or dynamic.	

7.6.3 Statistics

When enable and set GVRP function then administrator can check every port in GVRP include Receive / Transmit and Error information.





Click the "Clear" button to clear this page.

Receive	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	0
Transmit	
Join empty	0
Empty	0
Leave Empty	0
Join In	0
Leave In	0
Leave All	188

Error	
Invalid Protocol ID	0
Invalid Attribute Type	0
Invalid Attribute Value	0
Invalid Attribute Length	0
Invalid Event	0



Field	Description			
Join empty	The number of Receive or Transmit Join empty attribute value.			
Empty	The number of Receive or Transmit Empty attribute value.			
Leave Empty	The number of Receive or Transmit Leave Empty attribute value.			
Join In	The number of Receive or Transmit Join In attribute value.			
Leave In	The number of Receive or Transmit Leave In empty attribute value.			
Leave All	The number of Receive or Transmit Leave All attribute value.			
Invalid Protocol ID	The number of Receive Invalid Protocol ID			
Invalid Attribute Type	The number of Receive Invalid Attribute Type			
Invalid Attribute Value	The number of Receive Invalid Attribute value.			
Invalid Attribute Length	The number of Receive Invalid Attribute Length.			
Invalid Event	The number of Receive Invalid Event.			







8. MAC Address Table

8.1 Dynamic Address

This page can display MAC address for connected device. Administrator can set aging time for connected port.

MAC Address Table → Dy	ynamic A	Addres	S		
♦ Network		Aging T	ime 300		Soc (10, 620, default 2)
✤ Port		Aging T			Sec (10 - 630, default 3
✤ POE Setting			1		
* VLAN		Apply	J		
- MAC Address Table					
Dynamic Address Static Address Filtering Address			v entries SI	howing 1 to 1	15 of 15 entries
Port Security Address					~
Port Security Address Spanning Tree		VLAN	MAC Address	Port	~
 Spanning Tree 		VLAN 1	MAC Address 00:08:9B:D5:33:E4	Port GE25	~
Spanning TreeDiscovery					~
 Spanning Tree Discovery DHCP 			00:08:9B:D5:33:E4	GE25	~
 Spanning Tree Discovery DHCP 		1 1	00:08:9B:D5:33:E4 00:11:32:11:76:30	GE25 GE25	~

Aging Time : The time in seconds that an entry remains in the MAC address table. Its valid range is from 10 to 630 seconds, and the default value is 300 seconds.

Click the "Apply" button to save your changes settings.

Field	Description
MAC Address	The MAC address to which packets will be statically forwarded.
VLAN	Specify the VLAN to show or clear MAC entries.
Port	Interface or port number.

When administrator select checkbox MACs address and click "Add Static Address" button then selected MAC address will move to "Static Address" function.





Static Address 8.2

If administrator fixed an MAC address in the port then device MAC address will bind in the port, if device connection other port will can't working only connection bind port, Setting "add" and "Edit" and "Delete" function for this management.

MAC Address Table 🔿 Stat	tic Address
✤ Network	Static Address Table
∗ Port	
✤ POE Setting	Showing All entries Showing 1 to 1 of 1 entries
	VLAN MAC Address Port
 MAC Address Table 	4094 8C:4D:EA:00:00:01 GE2
Dynamic Address Static Address Filtering Address Port Security Address	Add Edit Delete

Field	Description	
MAC Address	The MAC address to which packets will be statically forwarded.	
VLAN	Specify the VLAN to show or clear MAC entries.	
Port	Interface or port number.	

C Address	8C:4D:EA:00:00:01		
VLAN	4094	(1 - 4094)	
Port	GE1 V		

- > MAC Address : Enter the MAC address to which packets will be statically forwarded.
- \triangleright VLAN : Enter the Specify the VLAN ID
- \succ **Port :** Select an interface or port number.

Click the "Apply" button to save your changes or "Close" the button to close settings.

+(886) 2-8911-6160





Filtering Address 8.3

Administrator can set need filtering MAC address in the MAC table. If MAC is added on table this MAC will be blocked, Setting "add" and "Edit" and "Delete" function for this management.

MAC Address Table \mapsto Filtering Address				
✤ Status				
♦ Network	Filtering Address Table			
✤ Port				
✤ POE Setting	Showing All v entries Showing 1 to 1 of 1 entries Q			
✤ VLAN	VLAN MAC Address			
 MAC Address Table 	4094 8C:4D:EA:00:00:0E			
Dynamic Address	First Previous			
Static Address	Add Edit Delete			
Filtering Address				
Port Security Address				

Field Description				
MAC Address	Specify unicast MAC address in the packets to be dropped.			
VLAN	Specify the VLAN ID for the specific MAC address.			

Add Fi	Itering Addre	ss	
м	AC Address	8C:4D:EA:00:00:0E	
	VLAN	4094	(1 - 4094)
Apr	ply CI	ose	

- MAC Address : Enter to specify the unicast MAC address in the packets to be dropped. \geq
- \geq VLAN : Enter a VLAN ID that specifies a specific MAC address.

Click the "Apply" button to save your changes or "Close" the button to close settings.





Port Security Address 8.4

Administrator can set this Port Security Address function, Setting "add" and "Edit" and "Delete" function for this management.

MAC Address Table	t Security Addr	ess			
✤ Status					
♦ Network	Port Security	Address Tab	le		
✤ Port					
✤ POE Setting	Showing All 🗸	entries S	showing 1 to 1 of 1 en	tries	Q
★ VLAN		MAC Address	Туре	Port	
- MAC Address Table		C:4D:EA:00:08:0A	SecureConfigured	GE5	
Dynamic Address Static Address Filtering Address Port Security Address	Add	Edit	Delete	Fir	st Previous 1

Field	Description
VLAN	Specify the VLAN to show port security.
MAC Address	Specify the MAC address for port security.
Туре	Specify the Type for port security.
Port	Interface or port number.

C Address	8C:4D:EA:00:08:0A	
VLAN	4094	(1 - 4094)
Port	GE5 🗸	

- > MAC Address : Enter the MAC address for port security.
- VLAN : Enter the Specify the VLAN ID
- \succ Port : Select an interface or port number.

Click the "Apply" button to save your changes or "Close" the button to close settings.

+(886) 2-8911-6160



9. Spanning Tree

Spanning Tree function allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If Spanning Tree costs change, or if one network segment in the Spanning Tree becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

9.1 Property

Spanning Tree Property			
* Status			
♦ Network	State	Enable	
¥ Port		O STP	
≱ POE Setting	Operation Mode	RSTP	
¥ VLAN		O MSTP	
MAC Address Table	Path Cost	Long	
- Spanning Tree		O Short	
Property	BPDU Handling	 Filtering Flooding 	
Port Setting			
MST Instance MST Port Setting	Priority	32768	(0 - 61440, default 32768)
Statistics			
* Discovery	Hello Time	2	Sec (1 - 10, default 2)
* DHCP	Max Age	20	Sec (6 - 40, default 20)
✤ Multicast	Forward Delay	15	Sec (4 - 30, default 15)
IP Configuration	Tx Hold Count	e	(1 10 dofault 6)
✤ Security	IX Hold Count	6	(1 - 10, default 6)
¥ ACL			
¥ QoS	Region Name	8C:4D:EA:30:DD:53	
Diagnostics	Revision	0	(0 - 65535, default 0)
¥ Management	Мах Нор	20	(1 - 40, default 20)

- State: Administrator can choose Enable or Disable this function. \geq
- \geq Operation Mode: Administrator can choose use Spanning Tree (STP) or Rapid Spanning Tree (RSTP) or Multiple Spanning Tree (MSTP).
- \geq Path Cost: Administrator can choose STP judgment use Path cost for Long or Short.
 - **Long :** Specifies that the default port path costs are within the range: 1-200,000,000.
 - **Short:** Specifies that the default port path costs are within the range:1-65,535.
- \succ BPDU Handling: When the Switch receives the BPDU frame, Administrator can choose the BPDU Handling mode for Filtering or Flooding. Specify the BPDU forward method when the STP is disabled.

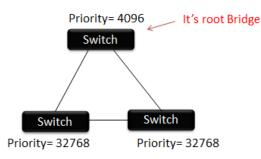
V1.0a



USER MANUAL



- **Filtering :** Filter the BPDU when STP is disabled.
- **Flooding :** Flood the BPDU when STP is disabled.
- Priority: Administrator can set bridge priority, default is 32768. The lower value (priority) is the root bridge. Specify the bridge priority. The valid range is from 0 to 61440, and the value should be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower value has the higher priority for the switch to be selected as the root bridge of the topology.



- Hello Time: The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.
- Max. Age / Forward delay : 2*(Forward Delay-1) >= Max Age >= 2*(Hello Time+1), the time interval in seconds for a switch to wait the configuration messages, without attempting to redefine its own configuration.
- Forward Delay : Specify the STP forward delay time, which is the amount of time that a port remains in the Listening and Learning states before it enters the Forwarding state. Its valid range is from 4 to 10 seconds.
- TX hold Count: Specify the tx-hold-count used to limit the maximum numbers of packets transmission per second. The valid range is from 1 to 10.
- Region Name: The MSTP instance name. Its maximum length is 32 characters. The default value is the MAC address of the switch.
- Revision: Administrator every time change MST value, customary "Revision" to add 1 value.
 The MSTP revision number. Its valid rage is from 0 to 65535.
- Max. Hop: Set max. hop of switch. Specify the number of hops in an MSTP region before the BPDU is discarded. The valid range is 1 to 40.





9.2 **Port Setting**

Spanning Tree	ort Setting									
 ✓ Status ✓ Network 		Dart C		Tabl	la					
♦ Network ♦ Port		Port Se	etting		le					
✤ POE Setting										
¥ VLAN		Er	ntry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge
MAC Address Table				GE1	Enabled	20000	48	Enabled	Enabled	Enabled
 Spanning Tree 	_		2 (GE2	Enabled	20000	48	Enabled	Enabled	Enabled
Property Port Setting		✓	3 (GE3	Enabled	20000	48	Enabled	Enabled	Enabled
MST Instance			4 (GE4	Enabled	20000	48	Enabled	Enabled	Enabled
MST Port Setting		~		GE5	Enabled	20000	48	Enabled	Enabled	Enabled
Statistics			6 (GE6	Disabled	20000	128	Disabled	Disabled	Disabled
Field	Descrip	otion								
Port	Specify	the in	terfa	ace I	D or the	list of int	terface	e IDs.		
State	The ope	The operational state on the specified port.								
Path Cost	STP pat	STP path cost on the specified port.								
Priority	STP pric	STP priority on the specified port.								
BPDU Filter	The sta	The states of BPDU filter on the specified port.								
BPDU Guard	The sta	The states of BPDU guard on the specified port.								
Operational Edge	The ope	The operational edge port status on the specified port.								
Operational Point-to-Point	The operational point-to-point status on the specified port.									
	The cur	rent p	ort r	ole	on the s	pecified p	oort. Tl	he possib	le values a	re:
Port Role	"Disable	"Disabled", "Master", "Root", "Designated", "Alternative", and Backup".								
Port State		The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".								
Designated Bridge	The brid	dge ID	oftl	he d	esignate	d bridge.				
Designated Port ID	The des	The designated port ID on the switch.								
Designated Cost	The pat	h cost	of t	he d	esignate	ed port or	n the s	witch		



Port	GE2-GE5,LAG1
State	C Enable
Path Cost	0 (0 - 20000000) (0 = Auto)
Priority	128 🗸
Edge Port	Auto Enable Disable
BPDU Filter	Z Enable
BPDU Guard	Enable
Point-to-Point	 Auto Enable Disable
Port State	Disabled
Designated Bridge	0-00:00:00:00:00
Designated Port ID	128-29
Designated Cost	20000
Operational Edge	False
Operational Point-to-Point	False

- State: Administrator can set Enable or Disable.
- Path Cost: Path Cost (1-20000000) This parameter is used determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short, the maximum path cost is 65,535. Range: 1-200000000, (set 0 = Auto, default is 0).
- Priority: If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. Range: 0-240, default is 128.
- **Edge Port:** Specify the edge mode..
 - Enable : Force to true state (as link to a host).
 - **Disable :** Force to false state (as link to a bridge).

In the edge mode, the interface would be put into the Forwarding state immediately upon link up. If the edge mode is enabled for the interface and there are BPDUs received on the

+(886) 2-8911-6160





interface, the loop might be occurred in the short time before the STP state change.

- **BPDU Filter :** The BPDU Filter configuration avoids receiving/transmitting BPDU from the \geq specified ports.
 - **Enable :** Enable BPDU filter function.
 - **Disable :** Disable BPDU filter function.
- \geq BPDU Filter : The BPDU Guard configuration to drop the received BPDU directly.
 - Enable : Enable BPDU guard function.
 - **Disable :** Disable BPDU guard function.
- \succ **Point-to-Point :** Specify the Point-to-Point port configuration:
 - Auto : The state is depended on the duplex setting of the port.
 - **Enable :** Force to true state.
 - Disable: Force to false state.
- \geq Port State : The current port state on the specified port. The possible values are : "Disabled", "Discarding", "Learning", and "Forwarding".
- \geq **Designated Bridge :** The bridge ID of the designated bridge.
- \geq Designated Port ID : The designated port ID on the switch.
- \geq Designated Cost : The path cost of the designated port on the switch.
- \succ **Operational Edge :** Show the "false" and "true" status.
- \geq Operational Point-to-Point : Show the "false" and "true" status.

Click the "Apply" button to save your changes or "Close" the button to close settings.

9.3 **MST Instance**

MST can have multiple sets of STP instances. Each instance is independently formed as a logical spanning tree. And instance has its own VLAN and port state, can independently set the priority of each port.





Status									
Network	MS	l'Insta	nce Tab	le					
Port									
POE Setting								a	
VLAN		MSTI	Priority	Bridge Identifiter	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
MAC Address Table	0	0	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	1-4094
Spanning Tree	0	1	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Property	0	2	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Port Setting	0	3	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
MST Instance	0	4	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
MST Port Setting Statistics	0	5	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Discovery	0	6	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
DHCP	0	7	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Multicast	0	8	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00	N/A	0	0	
IP Configuration	0	9	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Security	0	10	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
ACL	0	11	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
QoS	0	12	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Diagnostics	0	13	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
Management	0	14	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	
managomont	0	15	32768	32768-8C:4D:EA:30:DD:53	0-00:00:00:00:00:00	N/A	0	0	

Field	Description						
MSTI	MST instance ID.						
Priority	The bridge priority on the specified MSTI.						
Bridge Identifier	The bridge identifier on the specified MSTI.						
Designated Root Bridge	The designated root bridge identifier on the specified MSTI.						
Root Port	The designated root port on the specified MSTI.						
Root Path Cost	The designated root path cost on the specified MSTI.						
Remaining Hop	The configuration of remaining hop on the specified MSTI.						
VLAN	The VLAN configuration on the specified MSTI.						



MSTI	3
VLAN	Available VLAN Selected VLAN 2 1 3 5 4 5 6 7 8 9 10 •
Priority	32768 (0 - 61440, default 32768)
Bridge Identifiter	32768-8C:4D:EA:30:DD:53
Designated Root Bridge	0-00:00:00:00:00
Root Port	
Root Path Cost	0
Remaining Hop	0

- VLAN : Select the VLAN list for the specified MSTI. \geq
- \geq Priority: Specify the bridge priority on the specified MSTI. The valid range is from 0 to 61440, and the value must be the multiple of 4096. It ensures the probability that the switch is selected as the root bridge, and the lower values has the higher priority for the switch to be selected as the root bridge of the STP topology.
- \geq Bridge Identifier: Displays the priority and MAC address of the Root Bridge for the selected MST instance.
- \geq Root Port: Displays the root port of the selected MST instance.
- \geq **Root Path Cost:** Displays the root path cost of the selected MST instance.
- \geq **Remaining Hops:** Displays the number of hops remaining to the next destination.

Click the "Apply" button to save your changes or "Close" the button to close settings.

MST Port Setting 9.4

MST (Multiple Spanning Tree) is an extension to RST (Rapid Spanning Tree). MST further develops the usefulness of VLANs. MST configures a separate spanning tree for each VLAN group and blocks all but one possible alternate path within each spanning tree. A Multiple Spanning Tree Instance (MSTI) calculates and builds a loop-free topology to bridge packets from the VLANs that map to the instance.



Spanning Tree → MST Port Setting

✓ Network	MST	Port S	Setting	g Table							
✤ Port											
✤ POE Setting	MSTI	0 🗸									
* VLAN											
 MAC Address Table 		Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Туре	Designated Bridge	Designate
 Spanning Tree 		1	GE1	20000	48	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	48-1
Property		2	GE2	20000	48	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	48-2
Port Setting MST Instance		3	GE3	20000	48	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	48-3
MST Port Setting		4	GE4	20000	48	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	48-4
Statistics		5	GE5	20000	48	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	48-5
* Discovery		6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6
* DHCP		7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7
✤ Multicast		8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8
✤ IP Configuration		9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9
* Security		10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10
* ACL		11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11

MST Port Settings is used to configure the port MSTP settings for every MST instance. It is also used to view statistics that have been learned from the protocol.

Field	Description						
MSTI	Specify the port setting on the specified MSTI						
Port	Specify the interface ID or the list of interface IDs.						
Path Cost	The port path cost on the specified MSTI.						
Priority	The port priority on the specified MSTI.						
Port Role	The current port role on the specified port. The possible values are: "Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".						
Port State	The current port state on the specified port. The possible values are: "Disabled", "Discarding", "Learning", and "Forwarding".						
Mode	The operational STP mode on the specified port.						
Туре	 The possible value for the port type are: Boundary: The port attaching an MST Bridge to a LAN that is not in the same region. Internal: The port attaching an MST Bridge to a LAN that is not in the same region. 						
Designated Bridge	The bridge ID of the designated bridge.						



Designated Port ID	The designated port ID on the switch.
Designated Cost	The path cost of the designated port on the switch.
Remaining Hop	The remaining hops count on the specified port.

Edit MST Port Setting

MSTI	0
Port	GE6-GE7
Path Cost	0 (0 - 20000000) (0 = Auto)
Priority	128 🗸
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Туре	Boundary
Designated Bridge	0-00:00:00:00:00
Designated Port ID	128-6
Designated Cost	20000
Remaining Hop	20
Apply Close	

- MTSI : Specify the port setting on the specified MSTI.
- Port : Specify the interface ID or the list of interface IDs..
- Path Cost: Specify the STP port path cost on the specified MSTI,Path cost default value is 0 (auto) depends on source device rate.

If network is a loop occurs, the MST uses cost when selecting an interface to put in the forwarding state. Administrator can assign lower cost values to interfaces that you want selected first and higher cost values that you want selected last. If all interfaces have the same cost value, the MST puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces.

- Priority: Specify the STP port priority on the specified MSTI, Administrator can configure the MTP priority and make it more likely that the switch will be chosen as the root switch.
- Port Role: Displays the port role per instance, assigned by the MSTP algorithm to provide STP paths. The current port role on the specified port. The possible values are :





"Disabled", "Master", "Root", "Designated", "Alternative", and "Backup".

- Port State: The current port state on the specified port. The possible values are:
 "Disabled", "Discarding", "Learning", and "Forwarding".
- > Mode: The operational STP mode on the specified port.
 - **RSTP:** RSTP is enabled on the port.
 - **STP:** Classic STP is enabled on the port.
 - MSTP: MSTP is enabled on the port.
- **Type :** Displays the MSTP type of the port. The possible value for the port type are :
 - **Boundary :** The port attaching an MST Bridge to a LAN that is not in the same region.
 - Internal: The port attaching an MST Bridge to a LAN that is not in the same region.
- Designated Bridge: Displays the bridge ID number that connects the link or shared LAN to the root.
- Designated Port ID: Displays the priority and port ID on the designated bridge that connects the link or the shared LAN to the root.
- Designated Cost: Displays the cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Remaining Hops :** Displays the hops remaining to the next destination.

Click the "Apply" button to save your changes or "Close" the button to close settings.

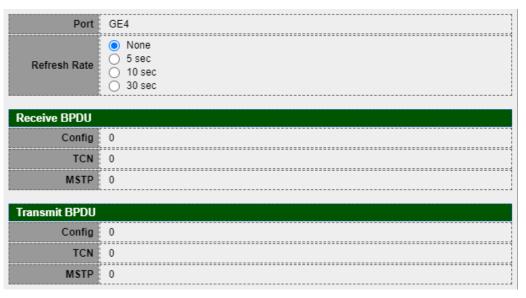
9.5 Statistics

This page can check Receive / Transmit BPDU information of the STP Port.

Spanning Tree → Statistic * Status	s									
* Network	s	tatistic	s Tabl	е						
✤ Port				_						
✤ POE Setting	R	efresh Ra	ite 0	✓ sec						
* VLAN										
 MAC Address Table 		-			Rec	eive BP	DU	Tran	smit BF	טסי
- Spanning Tree		Entr	y Po	Co	nfig	TCN	MSTP	Config	TCN	MSTP
Property		~	1 GE	1	0	0	0	0	0	0
Port Setting MST Instance		~	2 GE	2	0	0	0	0	0	0
MST Port Setting		~	3 GE	3	0	0	0	0	0	0
Statistics			4 GE	1	0	0	0	0	0	0
✤ Discovery			5 GE	5	0	0	0	0	0	0
* DHCP			6 GE	6	0	0	0	0	0	0
✤ Multicast			7 GE	7	0	0	0	0	0	0



Field	Description
Refresh Rate	The option to refresh the statistics automatically.
Receive BPDU (Config)	The counts of the received CONFIG BPDU.
Receive BPDU (TCN)	The counts of the received TCN BPDU.
Receive BPDU (MSTP)	The counts of the received MSTP BPDU.
Transmit BPDU (Config)	The counts of the transmitted CONFIG BPDU.
Transmit BPDU (TCN)	The counts of the transmitted TCN BPDU.
Transmit BPDU (MSTP)	The counts of the transmitted MSTP BPDU.
Clear	Clear the statistics for the selected interfaces
View	View the statistics for the interface.



- Refresh Rate : The option to refresh the statistics automatically : None , 5 sec , 10 sec , 30sec for refresh level.
- Clear : Clear the statistics for the selected interfaces.



10. Discovery(LLDP)

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet.

LLDP information is sent by devices from each of their interfaces at a fixed interval, in the form of an Ethernet frame. Each frame contains one LLDP Data Unit (LLDPDU). Each LLDPDU is a sequence of type-length-value (TLV) structures.

10.1 Property

Discovery → LLDP → Property			
* Network			
* Port	State	Enable	
✤ POE Setting		O Filtering	
* VLAN		Bridging Flooding	
* MAC Address Table		Flooding	
* Spanning Tree TLV Advertise	Interval	30	Sec (5 - 32767, default 30)
- Discovery Hold N	Aultiplier	4	(2 - 10, default 4)
LLDP Reinitializir Property	ng Delay	2	Sec (1 - 10, default 2)
Ded Oatling	nit Delay	2	Sec (1 - 8191, default 2)
MED Port Setting Packet View			
Local Information Fast Start Repe	at Count	3	(1 - 10, default 3)
Neighbor Statistics Apply			

- State: Administrator can choose Enable or disable this LLDP function.
- LLDP Handing: If cancel checkbox then administrator can choose Filtering / Bridging / Flooding for LLDP handing. Select LLDP PDU handling action to be filtered, bridging or flooded when LLDP is globally disabled
 - Filtering: Deletes the packet.
 - Bridging: (VLAN-aware flooding) Forwards the packet to all VLAN members.
 - Flooding: Forwards the packet to all ports
- TLV Advertise Interval: Select the interval at which frames are transmitted. (range 5-32760, default is 30)
- Hold Multiplier: Set Hold value (Range 2-10, default is 4). Administrator can control the aging time of local information on the neighbor device by configuring the value of the Hold multiplier. TTL=Hold multiplier * TLV Advertise Interval.
- Reinitializing Delay: S Select the delay before a re-initialization (range 1–10 seconds, default = 2)..





- \succ Transmit Delay: Select the delay after an LLDP frame is sent (range 1-8191 seconds, default = 3).
- Fast Start Repeat Count: The fast start repeat count when port link up(range 1–10, default = 3). \succ

Click the "Apply" button to save your changes settings.

10.2 Port Setting

Administrator can configure each port of the LLDPDU Transmit / Receive / Normal or Disable the mode and choose from "Optional TLV" list send the TLV type of port.

Discovery → LLDP → Por	t Setting	g			
ℽ Network	Port	Settin	ig Tab	le	
≽ Port					
✤ POE Setting					Q 🗌
* VLAN		Entry	Port	Mode	Selected TLV
MAC Address Table		1	GE1	Receive	Port Description , 802.3 MAC-PHY , 802.3 Maximum Frame Size , 802.1 PVID , 802.1 VLAN N
 Spanning Tree 		2	GE2	Receive	Port Description , 802.3 MAC-PHY , 802.3 Maximum Frame Size , 802.1 PVID , 802.1 VLAN N
– Discovery		3	GE3	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID ,
☆ LLDP		4	GE4	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID ,
Property		5	GE5	Normal	802.3 Link Aggregation , 802.3 Maximum Frame Size , Management IP Address , 802.1 PVID ,
Port Setting		6	GE6	Normal	$802.3 \ {\rm Link} \ {\rm Aggregation}$, $802.3 \ {\rm Maximum} \ {\rm Frame \ Size}$, ${\rm Management} \ {\rm IP} \ {\rm Address}$, $802.1 \ {\rm PVID}$,
MED Network Policy		7	GE7	Transmit	Port Description , System Description , 802.3 MAC-PHY , 802.1 PVID , 802.1 VLAN Name
MED Port Setting Packet View		8	GE8	Transmit	Port Description , System Description , 802.3 MAC-PHY , 802.1 PVID , 802.1 VLAN Name
Local Information		9	GE9	Transmit	Port Description , System Description , 802.3 MAC-PHY , 802.1 PVID , 802.1 VLAN Name
Neighbor		10	GE10	Normal	802.1 PVID
Statistics		11	GE11	Normal	802.1 PVID

Field	Description
Port	Display the port of LLDP state.
Mode	Display the Transmit (TX Only),Receive (RX Only),Normal (TX And RX),Disable
Selected TLV	Display the TLVs for your selected.







Port	GE7-GE9		
Mode	 Transmit Receive Normal Disable 		
Optional TLV	Available TLV System Name System Capabilities 802.3 Link Aggregation 802.3 Maximum Frame Size Management IP Address	Selected TLV 802.1 PVID System Description 802.3 MAC-PHY Port Description	*
802.1 VLAN Name	Available VLAN	Selected VLAN	×

- Mode : Administrator can choose Transmit(TX) / Receive(RX) or Normal(TX+RX) and Disable, if \geq choose disable will don't send and receive LLDPDU.
 - Transmit (TX Only): Transmit LLDP PDUs only.
 - Receive (RX Only): Receive LLDP PDUs only.
 - Normal (TX And RX): Transmit and receive LLDP PDUs both
 - Disable : Disable the transmission of LLDP PDUs
- \geq **Optional TLV :** Administrator can be configuration information into different TLV, encapsulates LLDPDU and issued to the neighbor device.
 - System Name
 - Port Description
 - System Description
 - System Capability
 - 802.3 MAC-PHY
 - 802.3 Link Aggregation
 - 802.3 Maximum Frame Size
 - Management Address
 - 802.1 PVID
- **802.1 VLAN Name :** Select the VLAN Name ID to be carried (multiple selection is allowed). \geq

Click the "Apply" button to save your changes or "Close" the button to close settings.





10.3 MED Network Policy

Administrator can see the display for LLDP MED Network Policy Setting, Setting "add" and "Edit" and "Delete" function for this management.

Discovery → LLDP → MEI	D Netw	ork Polic	y				
	MED) Network	Policy Tal	ole			
∗ Port							
✤ POE Setting	Show	ing All 🗸	entries	Showing	1 to 2 of 2 er	ntries Q	
* VLAN		Policy ID	Application	VLAN	VLAN Tag	Priority	DSCP
MAC Address Table		1	Voice	4094	Tagged	5	63
 Spanning Tree 		5	Guest Voice	4094	Tagged	2	11
– Discovery		•	Ouest voice	4004	lagged		
 LLDP Property Port Setting MED Network Policy MED Port Setting 		Add	Edit	Dele	ete	First	Previous

Field	Description
Policy ID	Display the policy ID.
Application	Display the network policy type.
VLAN	Display the VLAN ID.
VLAN Tag	Display the VLAN tag status.
Priority	Display the L2 priority.
DSCP	Display the DSCP value.





Policy ID	1 🗸	
Application	Voice	
VLAN	4094 Range (0 - 4095)	
VLAN Tag	 Tagged Untagged 	
Priority	5 •	
DSCP	63 🗸	

- Policy ID : Select specified network policy ID to configure.. \geq
- \geq **Application : S**elect the network policy application type.
 - Voice
 - Voice Signaling
 - Guest Voice
 - Guest Voice Signaling
 - Softphone Voice
 - Video Conferencing
 - App Streaming Video
 - **VideoSignaling**
- VLAN : Set the VLAN ID, range from 1 to 4094...
- \geq VLAN Tag : Set the VLAN tag status.
- \geq Select the network policy application type.
 - Tagged : Traffic is tagged.
 - Untagged : Traffic is untagged.
- **Priority :** Set the L2 priority, range from 0 to 7. \geq
- \geq **DSCP** : Set the DSCP value, range from 0 to 63.

Click the "Apply" button to save your changes or "Close" the button to close settings.





10.4 MED Port Setting

Administrator can see the display for LLDP MED Port Setting.

Discovery → LLDP → MH	D Port	Settin	g					
	ME	D Port	Settin	g Table				
¥ Port				-				
✤ POE Setting								
¥ VLAN		Entre	Dest	State	Netw	ork Policy	1	Incontant
MAC Address Table		Entry	Port	State	Active	Application	Location	Inventory
Spanning Tree		1	GE1	Enabled	Yes	Voice	No	Yes
– Discovery		2	GE2	Enabled	Yes	Voice	No	Yes
		3	GE3	Enabled	Yes	Voice	No	Yes
Port Setting		4	GE4	Enabled	Yes		No	No
MED Network Policy		5	GE5	Enabled	Yes		No	No
MED Port Setting		6	GE6	Enabled	Yes		No	No
Packet View		7	GE7	Enabled	Yes		No	No
Local Information Neighbor		8	GE8	Enabled	Yes		No	No
Statistics		9	GE9	Enabled	Yes		No	No

Field	Description
Port	Display the LLDP MED specified port.
State	Display the LLDP MED status
Optional TLV	Display the LLDP MED optional TLVs.
Network Policy	Display the LLDP MED network policy Active and Application IDs.
Location	Display the location status.
Inventory	Display the inventory by yes or no.





Port	GE1-GE3			
State	Enable			
	Available TLV	Selected	TLV	
Optional TLV	Location	Network		
		<u> </u>	•	
	Available Policy	Selected	Policy	
Network policy	5 (Guest Voice)	1 (Voice)	
		_		
Location				
Coordinate			(16 pairs of hexadecimal c	naracters)
Civic			(6 - 160 pairs of hexadecin	al characters)
ECS ELIN			(10 - 25 pairs of hexadecin	al characters)

- \succ **Port :** Select specified port or all ports to configure LLDP MED.
- \succ State : Select LLDP MED enable status
- \geq **Optional TLV :** Select LLDP MED optional TLVs (multiple selection is allowed).
 - Network Policy
 - Location
 - Inventory
- \geq Network Policy : Select the network policy IDs to be bound to ports. The network policy should be created in MED Network Policy page at first.
- \geq Location:
 - **Coordinate : Set Coordinate**
 - **Civic : Set Civic**
 - **ECS ELIN : Set ECS ELIN**

Click the "Apply" button to save your changes or "Close" the button to close settings.





10.5 Packet View

Administrator can select which port to view and click on the "Detail" button to view the information of the LLDP packet on the selected port.

Discovery ⇒ LLDP ⇒ Pa	cket Vie	w				
✤ Status	^					
✤ Network	Pac	ket Vie	w Tab	le		
✤ Port	-					
✤ POE Setting						Q
* VLAN		Entry	Port	In-Use (Bytes)	Available (Bytes)	Operational Status
MAC Address Table	0	1	GE1	162	1326	Not Overloading
 Spanning Tree 	0	2	GE2	162	1326	Not Overloading
– Discovery		3	GE3	200	1288	Not Overloading
☆ LLDP		4	GE4	113	1375	0
Property	0				1375	Not Overloading
Port Setting	0	5	GE5	113	1375	Not Overloading
MED Network Policy	0	6	GE6	113	1375	Not Overloading
MED Port Setting	0	7	GE7	81	1407	Not Overloading
Packet View Local Information	0	8	GE8	81	1407	Not Overloading

Field	Description
Port	Port Name
In-Use (Bytes)	Total number of bytes of LLDP information in each packet.
Available (Bytes)	Total number of available bytes left for additional LLDP information in each packet.
Operational Status	Overloading or not
Packet View Detail	
Port	GE5
Mandatory TLVs	
Size (Bytes)	21
Operational Status	Transmitted
MED Capabilities	
Size (Bytes)	9
Operational Status	Transmitted







MED Location	
Size (Bytes)	0
Operational Status	Transmitted
MED Network Policy	
Size (Bytes)	0
Operational Status	Transmitted
	i
MED Inventory	
Size (Bytes)	0
Operational Status	Transmitted
MED Extended Powe	r via MDI
Size (Bytes)	0
Operational Status	Transmitted
· · · · · · · · · · · · · · · · · · ·	
802.3 TLVs	
Size (Bytes)	19
Operational Status	Transmitted
Optional TLVs	
Size (Bytes)	40
Operational Status	Transmitted
802.1 TLVs	
Size (Bytes)	24
Operational Status	Transmitted
Total	
In-Use (Bytes)	113
III-Use (bytes)	113

Click the "Close" button to close the view detail page.

1375

Field	Description
Port	Port Name
	Total mandatory TLV byte size.
Mandatory TLVs	Status is sent or overloading.
	Total MED Capabilities TLV byte size.
MED Capabilities	Status is sent or overloading.

V1.0a

Available (Bytes)

Close





	Total MED Location byte size.
MED Location	Status is sent or overloading.
MED Network	Total MED Network Policy byte size.
Policy	Status is sent or overloading.
	Total MED Inventory byte size.
MED Inventory	Status is sent or overloading.
MED Extended	Total MED Extended Power via MDI byte
Power via MDI	size. Status is sent or overloading.
	Total 802.3 TLVs byte size.
802.3 TLVs	Status is sent or overloading.
	Total Optional TLV byte size.
Optional TLVs	Status is sent or overloading.
	Total 802.1 TLVs byte size.
802.1 TLVs	Status is sent or overloading.
Total	Total number of bytes of LLDP information in each packet.

10.6 Local Information

Displays switch summary and every port status of LLDP. Administrator can select which port to view and click on the "detail" button to view the information of the local device as well as the information of selected port LLDP property.

Status						
Network	Devic	e Summa	ary			
⊭ Port						
✓ POE Setting		Chassis I	D Subtype	MAC address		
⊧ VLAN		(Chassis ID	8C:4D:EA:30:D	D:53	
MAC Address Table		Sys	tem Name	Switch		
Spanning Tree	-	System D	escription	CS-2424G-24P)	
- Discovery	Su	upported C	apabilities	Bridge, Router		
LLDP Property		Enabled C				
Port Setting MED Network Policy			D Subtype			
MED Port Setting Packet View Local Information	Port S	Status Ta	ble			
Neighbor Statistics						Q
DHCP		Entry	Port	LLDP State	LLDP-MED State	
Multicast	0	1	GE1	Receive	Enabled	
IP Configuration	0	2	GE2	Receive	Enabled	





Device Summary

Field	Description
Chassis ID Subtype	Type of chassis ID, such as the MAC address.
Chassis ID	Identifier of chassis. Where the chassis ID subtype is a MAC address, the MAC address of the switch is displayed.
System Name	Name of switch.
System Description	Description of the switch.
Supported Capabilities	Primary functions of the device, such as Bridge, WLAN AP, or Router.
Enabled Capabilities	Primary enabled functions of the device.
Port ID Subtype	Type of the port identifier that is shown.

Port Status Table

Field	Description	
Port	Type of the port number	
LLDP Status	LLDP Tx and Rx abilities.	
LLDP Med Status	LLDP MED enable state.	

Click "detail" button on the page to view detail information of the selected port.





Local Information Detail

		Chassis ID		:4D:EA:30:DD:53
		System Name	Swi	<i>v</i> itch
	Syste	m Description	CS-	3-2424G-24P
	Supporte	d Capabilities	Brid	dge, Router
Enabled Capabilities		Brid	dge, Router	
Port ID		GE	1	
Port ID Subtype		Loc	cal	
Port Description				
ManagementAdd	rose Tablo			
Management Add	ress Table			
Address Subtype		Interface Sub		Interface Number

Management Address Table

Field	Description
Address	Type of the port number
Subtype	
Address	Display management IP address type.
Interface Subtype	Returned address most appropriate for management use, typically a Layer 3 address.
Interface number	Specific interface associated with this management address.

MAC/PHY Details

MAC/PHY Detail	
Auto-Negotiation Supported	True
Auto-Negotiation Enabled	True
Auto-Negotiation Advertised Capabilities	1000baseTFD , 100baseTXFD , 100baseTX , 10baseTFD , 10baseT
Operational MAU Type	Other





Field	Description
Auto-Negotiatio	Port speed auto-negotiation support status.
n Supported	
Auto-Negotiation	Port speed auto-negotiation active status.
Enabled	
Auto-Negotiation	Port speed auto-negotiation capabilities, for example, 1000BASE-T
Advertised	half-duplex mode, 100BASE-TX full-duplex mode.
Capabilities	
	Medium Attachment Unit (MAU) type. The MAU performs physical layer
Operational MAU	functions, including digital data conversion from the Ethernet interfaces'
	collision detection and bit injection into the network, for example,
	100BASE-TX full duplex mode.

802.3 Detail

02.3 Detail	
802.3 Maximum Frame Size	1522

Field	Description
802.3 Maximum	The maximum supported IEEE 802.3 frame size.
Frame Size	

802.3 Link Aggregation

802.3 Link Aggregation		
Aggreg	ation Capability N/A	
Ag	gregation Status N/A	
Agg	regation Port ID N/A	
Field	Description	
Aggregation Capability	Indicates whether the interface can be aggregated.	
Aggregation Status	Indicates whether the interface is aggregated.	
Aggregation Port	Advertised aggregated interface ID.	



MED Detail

MED Detail	
Capabilities Supported	Capabilities , Network policy
Current Capabilities	Capabilities , Network policy
Device Class	Network Connectivity
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A

Field	Description
Capabilities Supported	MED capabilities supported on the port.
Current Capabilities	MED capabilities enabled on the port.
Device Class	LLDP MED endpoint device class.
PoE Device Type	Port PoE type, for example, powered.
PoE Power Source	Port power source.
PoE Power Priority	Port power priority.
PoE Power Value	Port power value.
Hardware Revision	Hardware version.
Firmware Revision	Firmware version.
Software	Software version.

V1.0a

+(886) 2-8911-6160



RevisionSerial NumberDevice serial number.ManufacturerDevice chipset IC manufacturer name.NameDevice chipset IC model name.Model NameDevice chipset IC model name.Asset IDAsset ID.

Location Information

Location Information		
Civic	N/A	
Coordinate	N/A	
ECS ELIN	N/A	

Field	Description
Coordinate	Set Coordinate.
Civic	Set Civic.
ECS ELIN	Set ECS ELIN.

Network Policy Table

Application Type	VLAN	VLAN Type	Priority	DSCP
Voice	4094	Tagged	5	63

Field	Description	
Application	Display the network policy application type.	
	Voice	
	Voice Signaling	
	Guest Voice	
	Guest Voice Signaling	
	Softphone Voice	
	 Video Conferencing 	

+(886) 2-8911-6160



	 App Streaming Video 		
	 VideoSignaling 		
VLAN	Display the VLAN ID.		
VLAN Type	VLAN tag status. D isplay the network policy application Traffic is tagged or Traffic is untagged type.		
Priority	Display the L2 priority.		
DSCP	Display the DSCP value.		
ļ			

Click the "Close" button to close the information page.

10.7 Neighbor

The page displays information that was received using the LLDP protocol from neighboring devices. After timeout the information is deleted. (Based on the value received from the neighbor time to Live TLV during which no LLDP PDU was received from a neighbor), Setting **"add"** and "Edit" and **"Delete"** function for this management.

Discovery → LLDP → Neigh	ıbor							
* Status								
* Network	Neig	hbor Table	:					
✤ Port	01-	1 All			<i>(</i>)			
POE Setting	Snow	ing All 🗸 en	tries	Showing 1 to 3	of 3 entries		Q	
* VLAN		Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
MAC Address Table		GE25	MAC address	10:60:4B:8B:78:99	MAC address	10:60:4B:8B:78:99		2452
 Spanning Tree 		GE25	MAC address	00:E0:A0:10:04:6C	MAC address	00:E0:A0:10:04:6C		3397
– Discovery		GE27	MAC address	40:B0:34:54:97:82	MAC address	40:B0:34:54:97:82		3395
➢ LLDP Property Port Setting MED Network Policy MED Port Setting Packet View Local Information Neighbor		Clear	Refresh Detail]			First Previous	1 Next La
Statistics								

Field	Description
Local Port	Number of the local port to which the neighbor is connected.
Chassis ID Subtype	Type of chassis ID (for example, MAC address).
Chassis ID	Identifier of the 802 LAN neighboring device's chassis.



Port ID Subtype	Type of the port identifier that is shown.	
Port ID	Identifier of port.	
System Name Published name of the switch.		
	Time interval in seconds after which the information for this	
Time to Live	neighbor is deleted.	

Click "detail" to view selected neighbor detail information.

Neighbor Information Detail	
Local Port	GE25
Basic Detail	
Chassis ID Subtype	MAC address
Chassis ID	10:60:4B:8B:78:99
Port ID Subtype	MAC address
Port ID	10:60:4B:8B:78:99
Port Description	
System Name	
System Description	
Supported Capabilities	N/A
Enabled Capabilities	N/A
Management Address Table	
Address Subtype Address Interface Subt	ype Interface Number
0 results found.	

MAC/PHY Detail		
Auto-Negotiation Supported	True	
Auto-Negotiation Enabled	True	
Auto-Negotiation Advertised Capabilities	1000baseTFD	
Operational MAU Type	Other	



802.3 Power via MDI	
MDI Power Support Port Class	N/A
PSE MDI Power Support	N/A
PSE MDI Power State	N/A
PSE Power Pair Control Ability	N/A
PSE Power Pair	N/A
PSE Power Class	N/A
Power Type	N/A
Power Source	N/A
Power Priority	N/A
PD Request Power Value	N/A
PSE Allocated Power Value	N/A

802.3 Detail

802.3 Maximum Frame Size N/A

802.3 Link Aggregation		
Aggregation Capability	N/A	
Aggregation Status	N/A	
Aggregation Port ID	N/A	
802.1 VLAN and Protocol		
PVID		
VLAN Name	N/A	

MED Detail	
Capabilities Supported	Capabilities
Current Capabilities	Capabilities
Device Class	Endpoint Class 1
PoE Device Type	N/A
PoE Power Source	N/A
PoE Power Priority	N/A
PoE Power Value	N/A
Hardware Revision	N/A
Firmware Revision	N/A
Software Revision	N/A
Serial Number	N/A
Manufacturer Name	N/A
Model Name	N/A
Asset ID	N/A



		С	ivic N/A						
	Coordinat				N/A				
		EC \$ E	LIN N/A						
Network Policy 1									
Network Policy 1 Application Type				DSCP					

Click the "Close" button to close the information page.

10.8 Statistics

This page displays LLDP statistical information per port. The Link Layer Discovery Protocol (LLDP) Statistics page displays summary and per-port information for LLDP frames transmitted and received on the switch.

Status										
Network	Globa	al Stat	istics							
Port										
POE Setting	Ir	sertion	s 3							
VLAN		Deletion	s 0							
MAC Address Table		Drop	s 0							
Spanning Tree										
Discovery		AgeOut	s 0							
		tics T								
MED Port Setting Packet View Local Information Neighbor				Transmit Frame	R	eceive Frai	ne	Re	ceive TI V	Neighbor
Packet View Local Information		Entry	Port	Transmit Frame		eceive Fran			ceive TLV	Neighbor
Packet View Local Information Neighbor Statistics				Total	Total	Discard	Error	Discard	Unrecognized	Timeout
Packet View Local Information Neighbor Statistics DHCP		1	GE1	Total 0	Total 0	Discard 0	Error 0	Discard 0	Unrecognized 0	Timeout 0
Packet View Local Information Neighbor Statistics DHCP Multicast		1 2	GE1 GE2	Total 0 0	Total 0 0	Discard 0 0	Error 0 0	Discard 0 0	Unrecognized 0 0	Timeout 0 0
Packet View Local Information Neighbor Statistics DHCP Multicast IP Configuration		1 2 3	GE1 GE2 GE3	Total 0 0 0	Total 0 0 0 0	Discard 0 0	Error 0 0	Discard 0 0	Unrecognized 0 0	Timeout 0 0 0
Packet View Local Information Neighbor		1 2 3 4	GE1 GE2	Total 0 0	Total 0 0	Discard 0 0	Error 0 0	Discard 0 0	Unrecognized 0 0	Timeout 0 0

Global Statistics





Field	Description					
	The number of times the complete set of information advertised by a					
Insertions	particular MAC Service Access Point (MSAP) has been inserted into					
	tables associated with the remote systems.					
Deletions	The number of times the complete set of information advertised by MSAP has been deleted from tables associated with the remote systems.					
	The number of times the complete set of information advertised by					
Drops	MSAP could not be entered into tables associated with the remote					
	systems because of insufficient resources.					
	The number of times the complete set of information advertised by					
Age Outs	MSAP has been deleted from tables associated with the remote					
	systems because the information timeliness interval has expired.					

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.

C+	ati	cti	cs ⁻	Tal	hl	
JU	au	SU	LS	d	U	E

Field	Description
Port	Interface or port number.
Transmit Frame Total	Number of LLDP frames transmitted on the corresponding port.
Receive Frame	 Total: Number of LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled Discarded: Number of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. Errors: Number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Receive TLV	 Discarded: Number of TLVs of LLDP frames discarded for any reason by the LLDP agent on the corresponding port. Unrecognized: Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled Neighbor Timeout: Number of TLVs of LLDP frames that are unrecognied while the LLDP agent is enabled
Neighbor Timeout	Number of age out LLDP frames.





11. DHCP

The protocol operates on a client-server model. When DHCP clients connect to the network, they send broadcast queries to request the necessary information from the DHCP server. A DHCP server manages a pool of IP addresses and network configuration information. If they receive a query from a DHCP client, they will automatically be assigned an IP address and network parameters. Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol. It is used in Internet Protocol (IP) networks to dynamically distribute network configuration parameters. For example, a device can request an IP address for an interface from a DHCP server. Using DHCP also reduces the need for network administrators or users to manually configure these settings.

11.1 Property

Administrator can configure this "DHCP port Setting Table "for Enable / Disable DHCP Server function.

DHCP → Property					
	_				
* Network	-		S	tate 🔽 I	Enable
✤ Port		Statia D			
POE Setting		Static B	inding F	-irst 🔽 t	Enable
* VLAN	(Ar	un lu	1		
 MAC Address Table 		ply	ļ		
 Spanning Tree 					
* Discovery	DHCI	P Por	t Setti	ng Table	
– DHCP					0.5
Property					۹L
IP Pool Setting		Entry	Port	State	
VLAN IF Address Group Setting Client List		1	GE1	Enabled	
Client Static Binding Table		2	GE2	Enabled	
* Multicast		3	GE3	Enabled	
IP Configuration		4	GE4	Disabled	
		5	GE5	Disabled	

Use this section to enable the DHCP Server function on the switch. Also can select DHCP "Static Binding First" function to ticking "enable" for your configuration.

Click the "Apply" button to save your changes settings.

Field	Description
Port	Display the DHCP of port entry.





State	Show the DHCP Enable or DHCP Display Status.

Edit Port Setting :

You can select the port form GE1 - GE28 (Ports) and LAG1~LAG8 (Groups) to be set, and click "Edit" to edit DHCP port to ticking "enable" for your configuration.

E	lit Port Setting	
	Port GE12	
	State Cnable	
	Apply Close	

Click the "Apply" button to save your changes or "Close" the button to close settings.

11.2 IP Pool Setting

Administrator can configure this IP Pool Table Setting "add" and "Edit" and "Delete" function management.

DHCP → IP Pool Setting					
Network	IP Pool Ta	ble			
✤ Port					
POE Setting	Showing All	✓ entries	;		Showing 1 to
* VLAN			Section		
MAC Address Table	Pool	Section	Start Address	End Address	Gateway
 Spanning Tree 	□ adm	1	192,168,2,1	192.168.2.100	192.168.2.254
 Discovery 	adin		192.100.2.1	192.100.2.100	192.100.2.234
– DHCP	Add	Ed	lit Del	ete	
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table					





IP Pool Table						
Showing All 🗸 entries	Showing 1 to 1	l of 1 entries			9	
Pool Section section Start Address adm 1 192.168.2.1 192.168		Mask 255.255.255.0	DNS Primary Server	DNS Second Server	option 43 Address Format ascii	Lease time
Add Edit Delete					First Previous	1 Next La
Field	Description					
Pool	Display the I	Pool Nar	ne.			
Section	addres End Ad 	ddress : s pool co ldress : [Displays the onfigured for Displays the la	starting IP ad this DHCP ser ast IP address CP server insta	rver instance of the IP ad	е.
Gateway	Displays the server insta		gateway valu	e sent to clie	nts from thi	s DHCP
Mask	Displays the server insta		mask value se	ent to clients	from this DI	HCP
DNS Primary Server	Displays the DHCP server			value sent to	clients from	this
DNS Second Server	Displays the DHCP server		-	er value sent t	to clients fro	om this
Option43		•	ays of option ys of option 4	43 address. 43 format typ	e.	
Lease time	This field dis	splays th	e amount of t	time that the	IP address i	s valid.





Pool	adm
Gateway	192.168.2.254
Mask	255.255.255.0
	Section 1 🗸
IP Address Section	Start Address 192.168.2.1
	End Address 192.168.2.100
DNS Primary Server	C Enable 8.8.8.8
DNS Second Server	C Enable 168.95.1.1
option 43	● ascii ○ hex
Lease time	1 Day 00 ✔ Hour 00 ✔ Minute

- **Pool** : Select Add New Pool and enter a name for the DHCP Pool.
- Gateway : Enter the IP address of the gateway, which is the host on the LAN that relays all traffic coming into and going out of the LAN.
- Mask : Assign the subnet mask of IP address.
- > IP Address Section :
 - Section : Select the Section number.
 - **Start Address :** Enter the starting point for the DHCP server to assign IP address for the device connected.
 - End Address : Enter the ending point for the DHCP server to assign IP address for the device connected.
- **DNS Primary Server :** Select "enable" and fill in the for your primary DNS IP address.
- > **DNS Second Server :** Select "enable" and fill in the for your second DNS IP address.
- Option 43 : Configure option 43 character string with "ASCII" format and configure option 43 character string with "HEX" format in IP DHCP pool mode.
- Lease time : A controllable time period that DHCP server will reclaim IP addresses,Set the time value if set time is selected as Day / Hour / Minute.

Click the "Apply" button to save your changes or "Close" the button to close settings.





11.3 VLAN IF Address Group Setting

Administrator can configure select the drop down list Of "VLAN Interface" and ""DHCP server group " in the VLAN interface address pool table".

D	DHCP → VLAN IF Address Group Setting		
¥	Status	Vian Interface Address Pool Table	
¥	Network		
¥	Port	Interface VLAN 1 V	
¥	POE Setting	DHCP Server Group	
¥	VLAN		
¥	MAC Address Table	Apply	
¥	Spanning Tree		
¥	Discovery	DHCP Server Group Table	
-	DHCP		
	Property		9
	IP Pool Setting		
	VLAN IF Address Group Setting	Group ID Group IP Address Bind VLAN Interface	
	Client List	0 results found.	
	Client Static Binding Table		
¥	Multicast	Add Edit Delete	

- \succ Interface : Select a VLAN interface.
- \triangleright DHCP Sever Group : Select a DHCP Sever Group.

Click the "Apply" button to save your changes settings.

Administrator can configure this "DHCP Server Group Table "page setting for "add" and "Edit" and "Delete" function management.

Field	Description	
Group ID	Displays the DHCP Server Group ID	
Group IP Address	Displays the DHCP Server Group IP Address	
Bind VLAN Interface	Displays the DHCP Server Bind VLAN Interface	
DHCP Server Group Table		
DHCP Server Group		
Apply Close		



- \geq DHCP Server Group : Administrator can be select "DHCP Server Group in the drop-down box, and then confirm the grouping function to be set.
- **Group IP Address :** Administrator can fill in Group IP address. \succ

Click the "Apply" button to save your changes or "Close" the button to close settings.

11.4 Client List

This page can displayed DHCP Client List show" MAC Address Table" and show "IPv4 Address" and show "VLAN" and show "Hostname" information .

DHCP → Client List				
* Network	DHCP Client List			
✤ Port				
* POE Setting	Showing All 🗸 entries	Showing 0 t	o 0 of 0 e	entries Q
* VLAN	MAC Address Table	IPv4 Address	VLAN	Hostname
 MAC Address Table 			sults foun	ļ
 Spanning Tree 		0100		First Previous
* Discovery	Refresh			Flist Flevious
– DHCP	- Keirean			
Property				
IP Pool Setting				
VLAN IF Address Group Setting				
Client List				
Client Static Binding Table				

Field	Description	
MAC Address Table	Display the MAC address of the client device.	
IPv4 Address	Display the IP address sent to the client device.	
VLAN	Display the VLAN ID of the DHCP client.	
Hostname	Displays the hostname of the DHCP client.	

Click "Refresh" to refresh the "Client List" statistics .





11.5 Client Static Binding Table

Administrator can configure this "Static Binding Table "setting for "add" and "Delete" function management. And this page can displayed "Static Binding Table " show" MAC Address Table" and show "IPv4 Address" and show "VLAN" and show "User Name" information .

DHCP → Client Static Bind	ing Table			
 Status 				
 Network 	Static Binding Table			
✤ Port				
 POE Setting 	Showing All 🗸 entries	Showing 1 t	o 2 of 2 e	entries Q
* VLAN	MAC Address Table	IPv4 Address	VLAN	User Name
 MAC Address Table 	8C:4D:EA:00:00:01	192,168,2,88	4094	quest
 Spanning Tree 	8C:4D:EA:00:00:0E	192.168.2.85	4094	staff1
* Discovery	00.40.24.00.00.02	132.100.2.03	4034	
– DHCP	Add Delete			First Previous
Property IP Pool Setting VLAN IF Address Group Setting Client List Client Static Binding Table				

Field	Description
MAC Address Table	Display the MAC address of the client device.
IPv4 Address	Display the IP address sent to the client device.
VLAN	Display the VLAN ID of the DHCP client.
Users Name	Displays the Users Name of the DHCP client.

MAC Address	8C:4D:EA:00:08:0A	
VLAN	4094	(1 - 4094)
IPv4 Address	192.168.2.81	
User Name	service-PC	(1 - 32)



- \geq MAC Address : The MAC address of the device that wishes binding.
- \geq VLAN : Administrator can be configuration the DHCP VLAN ID.
- \geq IPv4 Address : The IP address that will assign to the device with Binding MAC address.
- \geq **User Name :** Generates a username for this binding rule.

Click the "Apply" button to save your changes or "Close" the button to close settings.

Multicast 12.

Multicast is the only type of IPv4 multicast that is supported by the Ethernet gateway.

12.1 General

12.1.1 Property

This page can be configured with unknown multicast action, administrator can set the forwarding method is based on the DMAC or the DIP, the function implements high performance data transfer from point to multipoint in network will be reduce the loading on the network.

Multicast → General → Property		
* Network	Flood	
♥ Port	Unknown Multicast	
 POE Setting 	Forward to Router Port	
* VLAN	Multicast Forward Method	
MAC Address Table		
Spanning Tree	IPv4 ODAC-VID DIP-VID	
Discovery	IPv6 DMAC-VID	
* DHCP	DIP-VID	
- Multicast		
☆ General	Apply	
Property Group Address		
Router Port		
Forward All		
Throttling		
Filtering Profile		
Filtering Binding		
IGMP Snooping		
MLD Snooping		
Ø MVR		

- \geq Unknown Multicast Action : Set the unknown multicast action
 - **Drop:** drop the unknown multicast data.
 - Flood: flood the unknown multicast data.
 - **Router port:** forward the unknown multicast data to router port.
- \geq Multicast Forward Method : Assign the subnet mask of IP address.
- \geq **IPV4**: Set the ipv4 multicast forward method.





- **MAC-VID**: forward method dmac+vid.
- **DIP-VID**: forward method dip+vid.
- > **IPV6 :** Set the ipv6 multicast forward method.
 - **MAC-VID**: forward method dmac+vid.
 - **DIP-VID**: forward method dip+vid(dip is ipv6 low 32 bit).

Click the "Apply" button to save your changes settings.

12.1.2 Group Address

The multicast address range is 224.0.0.0 to 239.255.255.255 and forms the Class D range which is made up of the high order bits 1110 followed by the 28 bit multicast group ID. There is no subletting with these Class D addresses. A multicast group can have a permanently-assigned address or the group may be Transient, , Setting **"add"** and **"Edit"** and **"Delete"** and **"Refresh"** function for this management.

Multicast ⇒ General ⇒ Gro	up Address
 Status 	
* Network	Group Address Table
✤ Port	
* POE Setting	IP Version IPv4 V
* VLAN	Showing All v entries Showing 0 to 0 of 0 entries
* MAC Address Table	
 Spanning Tree 	VLAN Group Address Member Type Life (Sec)
* Discovery	0 results found.
* DHCP	First Previ
– Multicast	Add Edit Delete Refresh
 General Property Group Address Router Port Forward All 	

- > **IPV4 Version :** Select the IP Version.
 - **IPv4 :** ipv4 multicast group.
 - **IPv6 :** ipv6 multicast group.

Field	Description
VLAN	The VLAN ID of group.
Group Address	The group IP address.



Member	The member ports of group.	
Туре	The type of group. Static or Dynamic.	
Life(Sec)	The life time of this dynamic group.	

Add Group Address	
VLAN	1•
IP Version	IPv4 🗸
Group Address	
Member	Available Port Selected Port GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8
Apply Clo	se

- VLAN : The VLAN ID of group. \geq
- > IP Version :
 - **IPv4 :** ipv4 multicast group.
 - **IPv6 :** ipv6 multicast group.
- Group Address : The group IP address. \geq
- \geq **Member :** The member ports of group.
 - Available Port: Optional port member.
 - Selected Port: Selected port member.

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.1.3 **Router Port**

A Multicast Router (MRouter) port is a port that connects to a Multicast router. The switch includes the MRouter port(s) when it forwards Multicast streams and IGMP/ MLD registration messages. It is required in order for all Router(s) can, in turn; forward the Multicast streams and propagate the registration messages to other subnets, Setting "add" and "Edit" and "Delete" function for this management.





Multicast 🕀 General 🖶 Router Port					
 Network 	Router Port Table				
✤ Port					
POE Setting	IP Version IPv4 V				
¥ VLAN	Showing All v entries Showing 1 to 1 of 1 entries				
MAC Address Table	ų				
Spanning Tree	VLAN Member Static Port Forbidden Port Life (Sec)				
Solution State	1 GE3 GE3				
* DHCP	First Previous				
– Multicast	Add Edit Refresh				
Property					
Group Address					
Router Port					
Forward All					

- > **IPV4 Version :** Select the IP Version.
 - **IPv4 :** ipv4 multicast router.
 - **IPv6 :** ipv6 multicast router.

Field	Description	
VLAN	The VLAN ID router entry.	
Member	Router Port member (include static and learned port member).	
Static Port	Static router port member.	
Forbidden Port	Forbidden router port member.	
Life(Sec)	The expiry time of the router entry.	



Add Router Port	t
VLAN	Available VLAN Selected VLAN
IP Version	IPv4 V
Туре	 Static Forbidden
Port	Available Port Selected Port GE1 Image: Constraint of the selected Port GE2 Image: Constraint of the selected Port GE3 Image: Constraint of the selected Port GE4 Image: Constraint of the selected Port GE5 Image: Constraint of the selected Port GE6 Image: Constraint of the selected Port GE8 Image: Constraint of the selected Port
Apply	Close

- VLAN : The VLAN ID of group. \succ
 - Available VLAN: Optional VLAN member.
 - Selected VLAN: Selected VLAN member.
- \geq **IP Version :**
 - **IPv4**: IPv4 multicast router.
 - **IPv6 :** IPv6 multicast router.

Type : The router port type:

- Static : Static router port.
- Forbidden : forbidden router port, can't learn dynamic router port member.
- \triangleright Port : The member ports of Router entry.
 - Available Port: Optional router port member.
 - Selected Port: Selected router port member.

Click the "Apply" button to save your changes or "Close" the button to close settings.





12.1.4 Forward All

Configure ports or LAGs to receive Multicast streams from a specific VLAN. Administrator can statically configure a port to Forward All if the devices connecting to the port do not support IGMP or MLD, Setting "add" and "Edit" and "Delete" function for this management.

Note	The configuration affects only the ports that are members of the selected VLAN.					
Multie	ast → General → For	ward All				
 Status 	ist of General of For					
* Networ	k	Forward All Table				
* Port		IP Version IPv4 at				
POE Se	etting	IP Version IPv4 V				
♦ VLAN		Showing All v entries Showing 1 to 1 of 1 entries O				
* MAC A	ddress Table	<u>ч</u>				
Spanni	ng Tree	VLAN Static Port Forbidden Port				
Discove	ery	□ 1 GE1				
* DHCP		First Pre				
- Multica	ast	Add Edit Delete				
la Gene						
	perty					
	oup Address uter Port					
	rward All					

- IPV4 Version : Select the IP Version. \geq
 - IPv4 : IPv4 multicast forward all.
 - IPv6 : IPv6 multicast forward all.

Field	Description	
VLAN	VLAN ID of forward all entry	
Static Port	Known multicast group always forward port member	
Forbidden Port	Known multicast group always not forward port member	





Add Forward All	
VLAN	Available VLAN Selected VLAN
IP Version	IPv4 V
Туре	 Static Forbidden
Port	Available Port Selected Port GE2 GE1 GE4 GE5 GE6 C GE7 C GE8 C
Apply	Close

- **VLAN :** The VLAN ID of forward all entry.
 - Available VLAN: Optional VLAN member.
 - Selected VLAN: Selected VLAN member.
- \geq **IP Version :**
 - IPv4 : IPv4 multicast forward all.
 - IPv6 : IPv6 multicast forward all.
- **Type :** The forward all port type \geq
 - Static : Static forward all port. The port is statically configured as a Multicast router port.
 - Forbidden : Forbidden forward all port. This port is not to be configured as a Multicast Router port, even if IGMP or MLD queries are received on this port.
- \geq Port : The member ports of forward all.
 - Available Port: Optional router port member.
 - Selected Port: Selected router port member.

Click the "Apply" button to save your changes or "Close" the button to close settings.





Throttling 12.1.5

This page allow user to configure port can learned max group number and if port group number arrived max group number action.

Multicast 🖻 General 🖶 Throttling						
* Network	Throttling Table					
✤ Port	IP Version IPv4 V					
 POE Setting 						
* VLAN						
MAC Address Table	_	_		_		чL
 Spanning Tree 		Entry	Port	Max Group	Exceed Action	
* Discovery		1	GE1	256	Deny	
* DHCP		2	GE2	256	Deny	
– Multicast		3	GE3	256	Deny	
a General		4	GE4	256	Deny	
Property		5	GE5	256	Deny	
Group Address		6	GE6	256	Deny	
Router Port Forward All		7	GE7	256	Deny	
Throttling		8	GE8	256	Deny	

- IPV4 Version : Select the IP Version. \geq
 - **IPv4**: IPv4 for IGMP snooping throttling.
 - **IPv6**: IPv6 for MLD snooping throttling.

Field	Description
Port	Display the Port Name
Max Group	Display the Max number of group for port

Exceed Action Display the port exceed max number group learning group action

dit Throttling	
Port	GE14
IP Version	IPv4
Max Group	256 (0 - 256)
Exceed Action	Deny Replace
Apply Clo	se





- \geq **Port :** Display the selected port list.
- \geq **IP Version :** Display the selected IP version
- \geq **Max Group :** Max number of group for port
- \geq **Exceed Action :** Excess Max number of port learning group action.
 - Deny: do not learning group.
 - **Replace:** random replace one exist group.

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.1.6 **Filtering Profile**

Filter profile permits or denies a range of Multicast groups to be learned when the join group matches the filter profile IP group range, Setting "add" and "Edit" and "Delete" function for this management.

Multicast → General → Filt	tering Profile		
Network	Filtering Profile Table		
✤ Port			
 POE Setting 	IP Version IPv4 V		
* VLAN	Showing All v entries Showing 0 to 0 of 0 entries Q		
MAC Address Table			
 Spanning Tree 	Profile ID Start Address End Address Action		
* Discovery	0 results found.		
* DHCP	First Previous		
– Multicast	Add Edit Delete		
a General			
Property			
Group Address			
Router Port			
Forward All			
Throttling			
Filtering Profile			

- IPV4 Version : Select the IP Version.
 - **IPv4**: IPv4 for IGMP snooping profile.
 - **IPv6 :** IPv6 for MLD snooping profile.

Field	Description
Profile ID	Display profile ID





Start Address	The start group address of profile
End Address	The end group address of profile
Action	Display profile action

Profile ID	(1 - 128)
IP Version	[IPv4 v]
Start Address	
End Address	
Action	Allow Deny

- Profile ID: Profile ID. \geq
- \geq IP Version : Display the selected IP version
 - IPv4: IGMP snooping profile.
 - IPv6: MLD snooping profile.
- \geq Start Address: The start group address of profile.
- \succ End Address : The end group address of profile.
- \geq Action: The action of profile:
 - Allow: permit all packets that match the profile.
 - Deny: deny all packets that match the profile.

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.1.7 **Filtering Binding**

When the setting is completed of Filtering Profile, administrator can select ports to set filtering binding.





Multicast ⇒ General ⇒ F	filtering	Bindin	g			
* Network	Filt	tering B	inding	Table		
✤ Port						
* POE Setting	IP V	IP Version IPv4 V				
* VLAN						0.5
MAC Address Table	_	_				μ
 Spanning Tree 		Entry	Port	Profile ID		
* Discovery		1	GE1			
* DHCP		2	GE2			
– Multicast		3	GE3			
		4	GE4			
Property		5	GE5			
Group Address Router Port		6	GE6			
Forward All		7	GE7			
Throttling		8	GE8			
Filtering Profile		9	GE9			
Filtering Binding		10	GE10			

IPV4 Version : Select the IP Version. \geq

- **IPv4**: IPv4 for IGMP snooping throttling.
- **IPv6**: IPv6 for MLD snooping throttling.

Field	Description				
Entry	Entry of number				
Port	Port Name				
Profile ID	Port binding Profile ID				
Edit Filtering Bi	nding				
Port	GE1-GE3				
IP Version	IPv4				
Profile ID	Enable				

Close Apply

Port: Selected Port List.

- \succ **IP Version :** Display Selected Port filtering IP version.
- Profile ID: If check Enable, can select or change profile ID, Else it will delete port filter profile \geq binding.

Click the "Apply" button to save your changes or "Close" the button to close settings.

+(886) 2-8911-6160





12.2 IGMP Snooping

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic. The IGMP snooping support v2 & v3, administrator can forward or drop Unknown Multicast.

12.2.1 Property

When IGMP Snooping is enabled globally or on a VLAN, all IGMP packets are forwarded to the CPU. The CPU analyzes select of ports are asking to join Multicast groups on VLAN or routers that are generating IGMP queries, or receiving PIM / OSFP / DVMRP / IGMP query protocols incoming packets.

Multicast 🖶 IGMP Snooping	⇒ Property	y					
* Network	-	State 🔽 E	nable				
✤ Port			GMPv2				
* POE Setting		Version	GMPv3				
* VLAN	Report S	uppression 🔽 E	nable				
MAC Address Table							
 Spanning Tree 	Apply						
* Discovery							
* DHCP	VLAN Setti	ng Table					
– Multicast							
General							
			Router Port	Queru	Quant	Query May	Loot Mon
Property	VLAN	Operational Status		Query	Query	Query Max	Last Men
Querier			Auto Learn	Robustness	Interval	Response Interval	Query Cou
Statistics	1	Disabled	Enabled	2	125	10	
MLD Snooping	(1					
© MVR	Edit	J					

- \geq State: Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.
 - Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
- \geq Version: Select either IGMPv2 or IGMPv3,Set the igmp snooping version.
 - **IGMPv2:** Only support process igmp v2 packet.
 - IGMPv3: Support v3 basic and v2.
- \geq **Report Suppression:** Enable or disable IGMP report suppression. If administrator select disabling this feature will forward all IGMP reports to Multicast routers, Set the enabling status of IGMP v2 report suppression.
 - **Enable:** If Checked Enable IGMP Snooping v2 report suppression, else Disable the report

V1.0a

+(886) 2-8911-6160





suppression function. Click the "Apply" button to save your changes.

VLA	N Setti	ng Table							
								Q _	
	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
	1	Disabled	Enabled	2	125	10	2	1	Disabled
	Edit]							

Field	Description
VLAN	The IGMP entry VLAN ID
Operation Status	The enable status of IGMP snooping VLAN functionality
Router Port Auto Learn	The enabling status of IGMP snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Last Member Query count	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive IGMP Leave message.

V1.0a





VLAN	1		
State	🗹 Enable		
Router Port Auto Learn	Enable		
Immediate leave	Enable		
Query Robustness	2	(1 - 7, default 2)	
Query Interval	125	Sec (30 - 18000, default 125)	
Query Max Response Interval	10	Sec (5 - 20, default 10)	
Last Member Query Counter	2	(1 - 7, default 2)	
Last Member Query Interval	1	Sec (1 - 25, default 1)	
perational Status			
Status	Disabled		
Query Robustness	2		
Query Interval	125 (Sec)		
Query Max Response Interval	10 (Sec)		
Last Member Query Counter	2		
Last Member Query Interval	1 (Sec)		

- VLAN: The VLAN ID of IGMP Snooping.
- State: Set the enabling status of IGMP Snooping VLAN functionality. \geq
 - Enable: Enable: If Checked Enable IGMP Snooping VLAN, else is Disabled IGMP Snooping VLAN.
- \geq Router Port Auto Learn: Set the enabling status of IGMP Snooping router port learning.
 - Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
- \geq **Immediate leave:** Immediate Leave the group when receive IGMP Leave message.
 - Enable: If checked Enable immediate leave, else disable immediate leave.
- \geq Query Robustness: The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
- Query Interval: The Admin interval of querier to send general query. \geq
- \geq **Query Max Response Interval:** The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
- \geq Last Member Query Counter: The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
- \geq Last Member Query Interval: The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.



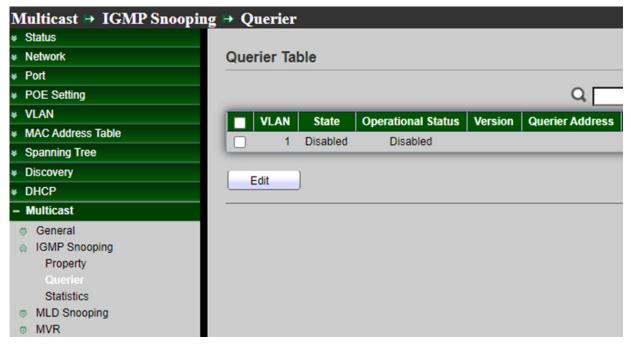


- > **Operational Status:** Set the enabling status of IGMP Snooping router port learning.
 - **Status:** Operational IGMP snooping status, must both IGMP snooping global and IGMP snooping enable the status will be enable.
 - Query Robustness: Operational Query Robustness.
 - **Query Interval:** Operational Query Interval.
 - Query Max Response Interval: Operational Query Max Response Interval.
 - Last Member Query Counter: Operational Last Member Query Count.
 - Last Member Query Interval: Operational Last Member Query Interval.

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.2.2 Querier

Administrator can choose created VLAN to enable or disable the IGMP Snooping query function. When select checkbox and click "**Edit**" button will be go to set IGMP Snooping version, this function can get IGMP Snooping query device regularly to VLAN local segments in all hosts and routers send IGMP Snooping general query packets, to the query segment which multicast group members.



Field	Description
VLAN	IGMP Snooping querier entry VLAN ID
State	The IGMP Snooping querier Admin State.

V1.0a





Operational Status	The IGMP Snooping querier operational status
Querier Version	The IGMP Snooping querier operational version.
Ouerier IP	The operational Querier IP address on the VI AN

Edit Querier	
VLAN	1
State	Enable
Version	O IGMPv2 IGMPv3
Apply	Close

- \geq VLAN: The Selected Edit IGMP Snooping querier VLAN List.
- State : Set the enabling status of IGMP Querier Election on the chose VLANs.
 - Enabled: if checked Enable IGMP Querier else Disable IGMP Querier.
- \geq Version : Set the query version of IGMP Querier Election on the chose VLANs.
 - IGMPv2: Querier version 2.
 - **IGMPv3:** Querier version 3. (IGMP Snooping version should be IGMPv3).

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.2.3 **Statistics**

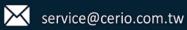
Display Receive / Transmit Packet information of IGMP snooping.





 Status 		
* Network	Receive Packet	
⊭ Port	Total	0
POE Setting	Valid	0
¥ VLAN	InValid	0
MAC Address Table		
Spanning Tree	Other	0
Discovery	Leave	0
* DHCP	Report	0
- Multicast	General Query	0
General	Special Group Query	0
 IGMP Snooping Property 	Source-specific Group Query	0
Querier Statistics	Transmit Packet	
MLD Snooping	Leave	0
ø MVR	Report	0
IP Configuration	General Query	0
Security	Special Group Query	0
# ACL	Source-specific Group Query	0
¢ QoS	Source-specific Group Query	
Diagnostics		

Field	Description
	 Total: Total RX igmp packet, include ipv4 multicast data to CPU.
	 Valid: The valid igmp snooping process packet.
	 InValid: The invalid igmp snooping process packet.
	• Other: The ICMP protocol is not 2, and is not ipv4
	multicast data packet.
Receive Packet	• Leave: IGMP leave packet.
	• Report: IGMP join and report packet.
	 General Query: IGMP General Query packet.
	• Special Group Query: IGMP Special Group General Query
	packet.
	 Source-specific Group Query: IGMP Special Source and
	Group General Query packet.
	• Leave: IGMP leave packet.
The second Decision	• Report: IGMP join and report packet.
Transmit Packet	 General Query: IGMP general query packet include
	querier transmit general query packet





- **Special Group Query:** IGMP special group query packet include querier transmit special group query packet.
- Source-specific Group Query: IGMP Special Source and Group General Query packet.

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.

12.3 MLD Snooping

The function support selective Multicast forwarding (IPv6), MLD Snooping must be enabled globally and for each relevant VLAN. The switch supports MLD Snooping on both static and dynamic VLANs. Hosts use the MLD protocol to report their participation in Multicast sessions, and the switch uses MLD Snooping to build Multicast membership lists. It uses these lists to forward Multicast packets only to switch ports where there are host nodes that are members of the Multicast groups. The switch does not support MLD Querier.

12.3.1 Property

Administrator to enable MLD Snooping in addition to the manually configured Multicast groups, the result is a union of the Multicast groups and port memberships derived from the manual setup and the dynamic discovery by MLD Snooping. However, only the static definitions are preserved when the switch is rebooted.

Multicast → MLD Snooping	Property	7					
* Network		State 🔽	Enable				1
✤ Port			VLDv1				
✤ POE Setting		Version	MLDv2				
¥ VLAN	Report	Suppression 🔽 I	Enable				
MAC Address Table							·····
 Spanning Tree 	Apply						
* Discovery							
* DHCP	VLAN Setti	ing Table					
– Multicast		ing lable					
 General IGMP Snooping MLD Snooping Property 	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Mem Query Cou
Statistics	□ 1	Disabled	Enabled	2	125	10	
ø MVR							
 IP Configuration 	Edit						

State: Administrator can select Enable or Un-enable, Set the enabling status of IGMP Snooping functionality.





- Enable: If Checked Enable IGMP Snooping, else is Disabled IGMP Snooping.
- **Version:** Select either MLDv1 or MLDv2, Set the MLD snooping version.
 - MLDv1: Only support process MLD v1 packet.
 - MLDv2: Support v2 basic and v1.
- **Report Suppression:** Set the enabling status of MLD v1 report suppression.
 - Enable: If Checked Enable MLD Snooping v1 report suppression, else Disable the report suppression function.

Click the "Apply" button to save your changes.

VLA	N Setti	ing Table							
								Q _	
ŀ	VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
	1	Disabled	Enabled	2	125	10	2	1	Disabled
	Edit]							

Field	Description
VLAN	The MLD entry VLAN ID
Operation Status	The enable status of MLD snooping VLAN functionality
Router Port Auto Learn	The enabling status of MLD snooping router port auto learning
Query Robustness	The Query Robustness allows tuning for the expected packet loss on a subnet.
Query Interval	The interval of querier to send general query
Query Max Response Interval	In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
Query Max Response Interval	The count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Last Member Query Interval	The interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
Immediate leave	The immediate leave status of the group will immediate leave when receive MLD Leave message.





Administrator can select VLAN in checkbox and click Edit button to set MLD Snooping.

VLAN	1
State	Enable
Router Port Auto Learn	Enable
Immediate leave	Enable
Querra De la strata	
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

- VLAN: The VLAN ID of MLD Snooping.
- \geq State: Set the enabling status of MLD Snooping VLAN functionality.
 - Enable: Enable: If Checked Enable MLD Snooping VLAN, else is Disabled MLD Snooping VLAN.
- \geq **Router Port Auto Learn:** Set the enabling status of MLD Snooping router port learning.
 - Enable: If checked Enable learning router port by query and PIM, DVRMP, else Disable the learning router port.
- \geq **Immediate leave:** Immediate Leave the group when receive MLD Leave message.
 - Enable: If checked Enable immediate leave, else disable immediate leave.
- \geq Query Robustness: The Admin Query Robustness allows tuning for the expected packet loss on a subnet.
- Query Interval: The Admin interval of querier to send general query. \geq
- \geq **Query Max Response Interval:** The Admin query max response interval, In Membership Query Messages, it specifies the maximum allowed time before sending a responding report in units of 1/10 second.
- \geq Last Member Query Counter: The Admin last member query count that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.
- \geq Last Member Query Interval: The Admin last member query interval that Querier-switch sends Group-Specific Queries when it receives a Leave Group message for a group.





- \geq **Operational Status:** Set the enabling status of MLD Snooping router port learning.
 - **Status:** Operational MLD snooping status, must both MLD snooping global and MLD snooping enable the status will be enable.
 - Query Robustness: Operational Query Robustness.
 - Query Interval: Operational Query Interval.
 - Query Max Response Interval: Operational Query Max Response Interval.
 - Last Member Query Counter: Operational Last Member Query Count.
 - Last Member Query Interval: Operational Last Member Query Interval.

12.3.2 **Statistics**

If administrator to enable MLD snooping, the page will display Receive / Transmit Packet information of MLD Snooping.

Multicast 🖻 MLD Snoopi	ng Statistics	
 Status 		
* Network	Receive Packet	
⊭ Port	Total	0
✤ POE Setting	Valid	0
♥ VLAN	InValid	0
MAC Address Table		
 Spanning Tree 	Other	0
 Discovery 	Leave	0
* DHCP	Report	0
– Multicast	General Query	0
General	Special Group Query	0
IGMP Snooping	Source-specific Group Query	0
 MLD Snooping Property 		
Statistics	Transmit Packet	
© MVR	Leave	0
 IP Configuration 	Report	0
 Security 	General Query	0
* ACL	Special Group Query	0
* QoS	Source-specific Group Query	0
 Diagnostics 		
 Management 		
	Clear Refresh	

Field	Description
	• Total: Total RX MLD packet, include ipv4 multicast data
	to CPU.
Receive Packet	 Valid: The valid MLD snooping process packet.
	 InValid: The invalid MLD snooping process packet.
	• Other: The ICMPV6 type is not MLD, and is not ipv6





	multicast data packet and is not IPV6 router protocol.
	• Leave: MLD leave packet.
	 Report: MLD join and report packet.
	 General Query: MLD General Query packet.
	 Special Group Query: MLD Special Group General
	Query packet.
	 Source-specific Group Query: MLD Special Source and
	Group General Query packet.
	• Leave: MLD leave packet.
	• Report: MLD join and report packet.
Transmit Packet	 General Query: MLD general query packet.
Transmit Packet	 Special Group Query: MLD special group query packet.
	 Source-specific Group Query: MLD Special Source and
	Group General Query packet.

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.

12.4 MVR

MVR (Multicast VLAN Registration) is designed for applications that use wide-scale deployment of multicast traffic across an Ethernet ring-based service-provider network (for example, the broadcast of multiple television channels over a service-provider network). MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

12.4.1 Property





Multicast MVR Property			
* Status			
* Network	State	Enable	
* Port	VLAN	1	
POE Setting			
* VLAN	Mode	 Compatible Dynamic 	
MAC Address Table			
Spanning Tree	Group Start	0.0.0.0	
* Discovery	Group Count	1	(1 - 128)
* DHCP	·····		
- Multicast	Query Time	1	Sec (1 - 10)
© General			
© IGMP Snooping Ope	erational Grou	цр	
MLD Snooping	Maximum	128	
	Current	0	
Property Port Setting	i.		
	oply		

- \geq State: Administrator can select Enable or Un-enable, Set the enabling status of MVR functionality.
 - **Enable:** if checked enable the MVR state, else disable the MVR state.
- \geq VLAN: Select the MVR VLAN ID.
- Mode: Set the MVR mode. \geq
 - **Compatible:** compatible mode.
 - **Dynamic:** dynamic mode, will learn group member on source port.
- \geq Group Start: Administrator can set range is 224.0.0.0 to 239.255.255.255, MVR group range start.
- Group Count: MVR group continue count, Uses the count parameter to configure a contiguous \geq series of MVR group addresses (the range for count is 1 to 128; the default is 1).
- \geq Query Time: MVR query time when receive MVR leave MVR group packet, Administrator can defines the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The value is in units of second. The range is 1 to 10, and the default is 1 second.
- \geq **Operational Group:**
 - Maximum: The max number of MVR group database.
 - **Current:** The learned MVR group current time.

Click the "Apply" button to save your changes settings.







12.4.2 **Port Setting**

Administrator can select ports to set role and immediate of MVR.

Multicast MVR Proper	rty		
 Status 	_		
Network	State	Enable	
✤ Port	VLAN	1	
POE Setting			
* VLAN	Mode	 Compatible Dynamic 	
MAC Address Table			
 Spanning Tree 	Group Start	0.0.0	
* Discovery	Group Count	1	(1 - 128)
* DHCP	dicup count	-	(1 120)
– Multicast	Query Time	1	Sec (1 - 10)
 General IGMP Snooping 	Operational Gro	up	
MLD Snooping	Maximum	128	
MVR Property Port Setting	Current	0	
Group Address	Apply		

Field	Description
Port	Port Name
Role	Port Role for MVR, the type is None/Receiver/Source

Immediate Leave Status of immediate leave

Edit Port Setting	
Port	GE1
Role	 None Receiver Source
Immediate Leave	Enable
Apply Close	2

- \succ **Port:** Display the selected port list.
- \succ Role: MVR port role.
 - None: port role is none.
 - **Receiver:** port role is receiver, Configures a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages. Receiver ports cannot belong to the multicast VLAN.
 - Source: port role is source, Configures uplink ports that receive and send multicast data as

V1.0a





source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch belong to the single multicast VLAN.

Note If administrator to set a non-MVR port with MVR characteristics is operation fails. The default configuration is as a non-MVR port.

- Immediate Leave: MVR Port immediate leave
 - **Enable:** if checked is enable immediate leave, else disable immediate leave, This function only be enabled on receiver ports to which a single receiver device is connected. When Enables the Immediate Leave feature of MVR on the port. The Immediate Leave feature is disabled by default

Click the "Apply" button to save your changes or "Close" the button to close settings.

12.4.3 Group Address

Setting "add" and "Edit" and "Delete" and "Refresh" function for this management.

Multicast → MVR → Group	p Address
 Network 	Group Address Table
✤ Port	
POE Setting	Showing All entries Showing 0 to 0 of 0 entries Q
♥ VLAN	VLAN Group Address Member Type Life (Sec)
MAC Address Table	0 results found.
 Spanning Tree 	First Previous
* Discovery	Add Edit Delete Refresh
* DHCP	
– Multicast	
Ø General	
IGMP Snooping	
MLD Snooping	
⊚ MVR	
Property	
Port Setting	
Group Address	

Field	Description
VLAN	The VLAN ID of MVR group.
Group Address	The MVR group IP address.





Member	The member ports of MVR group.
Туре	The type of MVR group. Static or Dynamic.
Life(Sec)	The life time of this dynamic MVR group.

VLAN	1	
Group Address	(0.0.0.0 - 0.0.0.0)	
Member	Available Port Selected Port	

- VLAN: The VLAN ID of MVR group. \geq
- \geq Group Address: MVR group IP address , Administrator can set MVR multicast group addresses on the switch. (The address range is 224.0.0.0 to 239.255.255.255)
- \succ Member: Select Ports in the MVR Group.
 - Available Port: Optional port member, it is only receiver port when MVR mode is compatible, it include source port when mode is dynamic.
 - Selected Port: Selected port member.

Click the "Apply" button to save your changes or "Close" the button to close settings.





IP Configuration 13.

By default all ports belong to the same VLAN and the switch only provides Layer 2 Function. To segment connected networks, first create a VLAN for each unique network user group or application traffic, assign all ports belonging to the same group to these VLANs, and assign an IP interface to each VLAN. By dividing the network into Different VLANs, which can be divided into subnets that are disconnected at the layer2. Network traffic within the same subnet is still switched using Layer 2 switching. and VLANs can now (as required) be interconnected with Layer 3 switching. Each VLAN represents a layer 3 virtual interface. You only need to provide Network address for each virtual interface, and traffic between different interfaces Subnets will be routed through Layer 3 switching.

13.1 IPv4 Management and Interfaces

This chapter describes how to configure the IP interface for management access Switch over the network. The switch supports IP version 4 and version 6, And can be managed simultaneously by any of these address types. You can manually configure specific IPv4 or IPv6 addresses, or instruct the switch to obtain an IPv4 address from a BOOTP or DHCP server. An IPv6 address can only be configured manually.

IPv4 Configuration – Set the IPv4 address for management access.

An IPv4 address default IP is '192.168.2.200' To configure a static address, To configure a static address, you need to change the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment (if no routing protocols are enabled). You can direct the device to obtain an address from a BOOTP or DHCP server, or manually configure a static IP address. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted.

13.1.1 **IPv4 Interface & Default IP Configure**

Administrator can configure this drop down list to specify the VLAN ID number of the IPv4 interface through which the IPv4 packets are forwarded and The Switch supports the VLAN interface type and Loopback interface type, Setting "add" and "Edit" and "Delete" function for this management.

V1.0a





IP Configuration → IPv4 M status	anagement and	Routing ⇒ II	Pv4 Interfac	e		
* Network	IPv4 Interfac	e Table				
* Port	IF V4 Internac	e lable				
POE Setting				Q		
* VLAN	Interface	IP Address Type	IP Address	Mask	Status	Roles
MAC Address Table	VLAN 1	Static	192.168.2.200	255.255.255.0	Valid	
 Spanning Tree 	VLANT	Static	192.108.2.200	255.255.255.0	valiu	primary
Discovery	Add]	Edit]	Delete			
¥ DHCP						
⊭ Multicast						
- IP Configuration						
 IPv4 Management and Routing IPv4 Interface IPv4 Routes 						
ARP						
IPv6 Management and Routing						

IPv4 Interface Table						
			Q			
Interface	IP Address Type	IP Address	Mask	Status	Roles	
VLAN 1	Static	192.168.2.200	255.255.255.0	Valid	primary	
Add	Edit De	lete				

Configure VLAN1 (Default VLAN) IP address for your POE Switch

And 'Save running configuration to startup configuration'

Interface	VLAN 1			
Address Type	 Dynamic Static 			
IP Address	192.168.2.200			
Mask	Network Mask	255.255.255.0		
Mask	O Prefix Length		(8 - 30)	
Roles	● primary ○ sub			

> Address Type :



- **Dynamic :** Select to set as "Dynamic" type.
- Static : Select to set as "Static" type.

If set the "Dynamic" type , The IP settings will be obtained from other DHCP Note server assignments.

- IP Address : IP Address of the VLAN. Valid IP addresses consist of four numbers, 0 to 255, \geq separated by periods. (Default IP is : 192.168.2.200).
- \succ Mask :
 - Network Mask : This mask identifies the host address bits used for routing to specific subnets. (Default Network Mask is : 255.255.255.0)

Prefix Length : In the Prefix Length field, define the Prefix Length of the Routing IPv4 Interface.

- \succ **Roles** :
 - **Primary :** In the Primary field, Select the setting defined as the primary roles.
 - Sub : In the Sub field, Select the setting defined as the secondary roles.

Click the "Apply" button to save your changes or "Close" the button to close settings.

'Save running configuration to startup configuration'

				Save	Logout	Reboot
IP Configuration ⇒ IPv4 1	Management and	Routing	Pv4 Interface			
	ID of last of a					
✤ Network ✤ Port	IPv4 Interface	e lable				
 ✓ POE Setting 				Q		
* VLAN		IP Address Type	IP Address	Mask	Status	Roles
MAC Address Table		Static	192,168,101,89	255.255.255.0	Valid	primary
 Spanning Tree 		Otatic	102.100.101.00	200.200.200.0	Valid	primary

After successfully changing the new IP, execute "Save running configuration to startup configuration" to make the new IP setting of POE Switch take effect every time it is started.





CERIO	CS-3424G-24P 24 Port Gigabit Managed PoE+ L2/L3 Lite Switch with 4 Combo Gigabit Ports Save Logout Reboot
IP Configuration -> IP	
System Information	
Logging Message	
© Port	
Link Aggregation MAC Address Table	Intra Iask Status Roles
NAC Address Table Network	
* Port	VL Save running configuration to startup 155.255.0 Valid primary configuration. Do you want to continue?
	Add
POE Setting	
* VLAN	OKCancel
MAC Address Table	
 Spanning Tree 	
* ERPS	

Click the "ok" button to save 'Save running configuration to startup configuration'.

Add New VLAN IP address setting on 'Loopback'

	O VLAN 1∨		
Interface	Loopback		
Address Type	DynamicStatic		
IP Address	192.168.182.8		
	Network Mask	255.255.255.0	
Mask	 Prefix Length 		(8 - 30)
Roles	 primary sub 		

- Address Type : The Interface for Loopback only provides settings as "static" type.
- > IP Address : In the IP Address field, define the IP address of the Routing IPv4 Interface.
- > Mask :

• **Network Mask :** In the Network Mask field, define the Subnet Mask of the Routing IPv4 Interface.

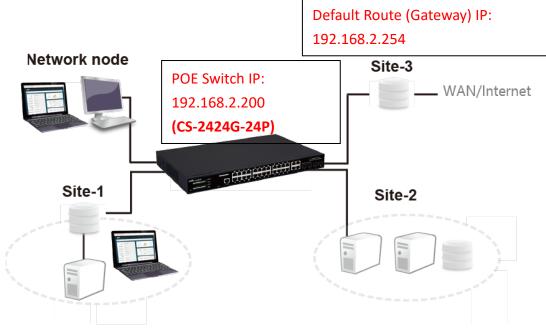
- **Prefix Length :** In the Prefix Length field, define the Prefix Length of the Routing IPv4
- Roles :
 - **Primary :** In the Primary field, Select the setting defined as the primary roles.
 - **Sub** : In the Sub field, Select the setting defined as the secondary roles.

Click the "Apply" button to save your changes or "Close" the button to close settings.



13.1.2 IPv4 Routes & Default Route Configure

You can enter static routes in the routing table using the IP > Static Routes (Add) page. Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology , so you should only configure a small number of stable routes to ensure network



The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. In the network, the router selects an appropriate path according to the destination address of the received data, and forwards the data to the next router. The last router in the path is responsible for forwarding the packet to the destination host.

For example, the traffic from "Network node" to the Internet through the Switch's default Route (default Gateway) (Site-3). You create one static route to connect to services offered by your ISP behind router (Site-2).

You create another static route to communicate with a separate network behind a router (Site-1)connected to the Switch.

Administrator can configure this "IPv4 Routing Table "page setting for **"add"** and "Edit" and **"Delete"** function management.





IP Configuration → IPv4 M	anagement and Routing	• 🖶 IPv4 Ro	utes	
✓ Status		,		
✤ Network	IPv4 Routing Table			
∗ Port				
✤ POE Setting				
∗ VLAN	Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address
 MAC Address Table 	162.159.200.0	24	Static	192,168,101,254
✤ Spanning Tree	192.168.101.0	24	Directly Connected	
✤ Discovery				
* DHCP	Add Edit	Delete		
✤ Multicast				
- IP Configuration				
IPv4 Interface				
IPv4 Routes				
ARP IPv6 Management and Routing				

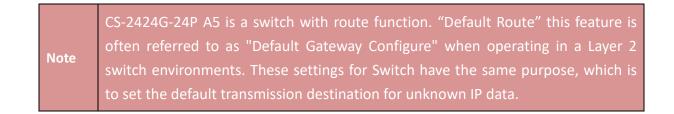
Configure next hop route of the Gateway IP forwarded packet in

"Default Route", for LAN device to access the Internet.

And 'Save running configuration to startup configuration'

Default routes in hosts are often called default gateways. The default gateway is usually a filtering device such as a NAT gateway router, firewall, or proxy server.

"Default route" is the route selected by the router when no other existing route can be found for the destination address in the IP packet. All packets whose destination is not in the router's routing table will use the default route. The route usually leads to another router that also handles the packet: if it knows how to route the packet, it forwards the packet to the known route; otherwise, the packet is forwarded to the default route. Route to another router. With each forwarding, the route increases the distance by one hop.



The default route in a TCP/IP network is a setting that tells the device how to forward the packet





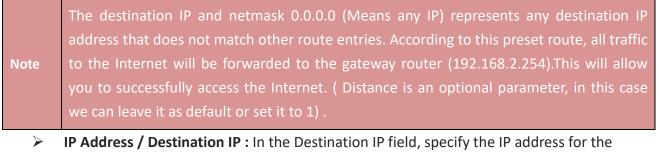
when the destination IP of the packet is not on the same subnet as the device, in order to achieve smooth access to the Internet. Use static routing settings to determine the gateway IP address to designate as the next hop.

Configure the "default route" (Gateway IP) of the POE switch. Please refer to the following.

Default Route (Gateway IP)Configure Sample:

IP Address	0.0.0.0	
Maak	Network Mask 0.0.0	.0
Mask	O Prefix Length	(0 - 32)
Next Hop Router IP Address	192.168.2.254	
Metric	1	(1 - 255, default 1)

The default route setting Sample destination IP address and Mask IP Address are "0.0.0.0 "(Means any IP), Gateway Router IP Address is "192.168.2.254", Metric is "1".



destination.

Mask :

- Network Mask : Specify the subnet mask for the attached network.
- Prefix Length : In the IPv4 Prefix Length field, specify the IPv4 prefix length for the destination.
- **Next Hop Router IP Address** : In the Next Hop IP Address field, specify the outgoing router \geq

V1.0a





IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

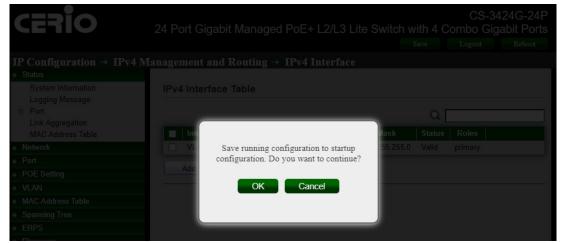
 \geq Metric : Please fill in the cost (hop count) of transmission you want to apply for routing purposes.

Click the "Apply" button to save your changes or "Close" the button to close settings.

'Save running configuration to startup configuration'

			Save	Logout	Reboot
IP Configuration → IPv4 Ma	anagement and Routing	g 🖶 IPv4 Ro	utes		
Network	IPv4 Routing Table				
¥ Port					
POE Setting					
¥ VLAN	Destination IP Prefix	Prefix Length	Route Type	Next Hop Rout	er IP Address
MAC Address Table		24	Static		
Spanning Tree	0.0.0.0 (Any IP)	24	Directly Connected	102.100.2.201	(Gateway IP
* Discovery	102.100.2.0	27	Directly Connected		
* DHCP	Add Edit	Delete			
 Multicast 					
- IP Configuration					
 IPv4 Management and Routing IPv4 Interface 					
IPv4 Routes					
ARP					
IPv6 Management and Routing					

After successfully changing the new IP, execute "Save running configuration to startup configuration" to make the Gateway IP setting of POE Switch take effect every time it is started.



Click the "ok" button to save 'Save running configuration to startup configuration'.

V1.0a



Static Route Configure Sample:

IP Address	162.159.200.1			
Maak	Network Mask	255.255.	255.0]
Mask	O Prefix Length			(0 - 32)
Next Hop Router IP Address	192.168.101.254			
Metric	2		(1 - 255, default 1)	

The Static Route Sample IP Address is 162.159.200.1 Gateway Router IP Address is 192.168.101.254

 \geq IP Address / Destination IP : In the Destination IP field, specify the IP address for the destination.

This parameter specifies the IP network address of the final destination. Routing is
always based on network numbers.
If you need to specify a route to a single host, use the subnet mask 255.255.255.255 in
the Subnet Mask field to force the network number to be the same as the host ID.

- Mask : \triangleright
- Network Mask : Specify the subnet mask for the attached network.
- Prefix Length : In the IPv4 Prefix Length field, specify the IPv4 prefix length for the destination.
- \geq **Next Hop Router IP Address** : In the Next Hop IP Address field, specify the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

The next router is always one of the adjacent neighbors or the IP address of the local Note

+(886) 2-8911-6160





Metric : Please fill in the cost (hop count) of transmission you want to apply for routing \succ purposes.

	This metric represents the "cost" of transmission for routing purposes. IP routing uses
	"hop count" as a measure of cost, with a minimum value of 1 for directly connected
Note	networks. Enter a number that approximates the cost of this link. The number does
	not need to be exact, but must be between 1 and 255. In fact, 1 or 2 or 3 is usually
	suggested here to fill in the frequently used numbers.

Click the "Apply" button to save your changes or "Close" the button to close settings.

Diagnostics 🔿 Ping		
		○ Hostname
≽ Port	Address Type	 IPv4
✤ POE Setting		O IPv6
* VLAN	Server Address	162.159.200.1
✓ MAC Address Table		
	Count	10 (1 - 32)
✤ Discovery	2	
* DHCP	Ping Sto	p
≽ Multicast		
	Ping Result	
★ Security	-	
* ACL		
¥ QoS	Packet Status	
– Diagnostics	Status	Success.
S Logging	Transmit Packet	10
Mirroring	Receive Packet	10
Ping Traceroute	Packet Lost	0 %

For the Static Route Sample IP Address Enter to "162.159.200.1", If the setting is successful, you can test and verify it through the "Diagnostics> Ping tool.





	IPv4 Routing Table							
							0.5	
l							ч L	
l		Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
I		162.159.200.0	24	Static	192.168.101.254	2	1	VLAN 1*
		192.168.101.0	24	Directly Connected				VLAN 1*
		Add] Edit	Delete					

Field	Description
Destination IP Prefix	The IP Prefix for the destination
Prefix Length	The prefix length for the active route.
Router Type	The type of route: Static or Dynamic, depending on how the route was added.
Next Hop Router IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router (ex. Your Gateway site IP address) is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Metric	The Metric value for the configured next hop. Specify the Metric (sometimes called administrative distance), which is an integer value from 1 to 255.
Administrative Distance	The route administrative distance of the configured route.
Outgoing Interface	The outgoing interface of the route active or inactive.





13.1.3 ARP

ARP (Address Resolution Protocol, Address Resolution Protocol) is a protocol that resolves an IP address into an Ethernet MAC address (or physical address). In a local area network, when a host or other network device has data to send to another host or device, it must know the other party's network layer and IP address. But just having an IP address is not enough, because IP data must be encapsulated into a frame to be sent through the physical network, so the sending station must also have the physical address of the receiving station, so the address needs to be mapped from the IP to the physical address. ARP is the protocol to achieve this function.

ARP table (ARP Cache page)

After the device resolves the destination MAC address through ARP, it will add an IP address-to-MAC address mapping entry in its own ARP table for subsequent data forwarding to the same destination. ARP table are divided into "dynamic ARP table" and "static ARP table".

Use the ARP Table (ARP Cache page) to view entries in the table, a table of the remote connections most recently seen by this switch.

IP Configuration → IPv4 M	anagement and	l Routing 并	ARP		
♦ Network	ADD E	ntry Age Out 12	00	Sec (15 - 21600, de	sfault (1200)
≽ Port				Sec (15 - 21000, de	nauit 1200)
FOE Setting		0	All Dynamic		
≠ VLAN	Clear ARP 1	able Entries	Static		
MAC Address Table		0	Normal Age Out		
Spanning Tree)			
Discovery	Apply	Cancel			
⊧ DHCP					
⊧ Multicast	ARP Table				
- IP Configuration					
					Q
IPv4 Interface	Interface	IP Address	MAC Address	Status	
IPv4 Routes	VLAN 1	192.168.101.63	00:e0:a0:10:04:6c	Dynamic	
ARP	U VLAN 1	192.168.101.100	8c:4d:ea:fe:05:be	Static	
IPv6 Management and Routing	VLAN 1	192.168.101.167	00:60:b9:bf:b6:74	Dynamic	
Security	VLAN 1	192.168.101.254	8c:4d:ea:04:f8:50	Dynamic	
ACL	-	17)		
¢ QoS	Add	Edit	Delete		

- \succ **ARP Entry Age Out :** The setting of ARP aging time can be set from 15 seconds to 21600 seconds, and the default is 1200 seconds.
- **Clear ARP Table Entries :** Administrator can configure this "ARP Table for Clean ARP Table \geq Entries by "All" and "Dynamic" and "Static" and by "Normal Age Out" (ARP aging set time) management.





1. Dynamic ARP Table : Dynamic ARP Table are automatically generated and maintained by the ARP protocol through ARP aging-out time , and can be outdated and invalid, updated by new ARP Note interface is disabled, the corresponding dynamic ARP Table will be deleted 2. Static ARP Table :

Click the "Apply" button to save your changes or "*Cancel*" the button to cancel settings.

ARP Table

Administrator can configure this "ARP "page setting for "add" and "Edit" and "Delete" function management.

Field	Description
Interface	The routing interface associated with the ARP entry.
IP Address	Displays the IP address of the device (on a subnet) that is attached an existing routing interface of the switch.
MAC Address	Displays the unicast MAC address of the attached device. The address is six two-digit hexadecimal numbers separated by colons, for example, 40:bo:34:54:97:82
Status	 The type of ARP entry. Possible values are as follows: Local : An ARP entry associated with one of the switch's routing interface's MAC addresses. Gateway : A dynamic ARP entry whose IP address is that of a router. Static : An ARP entry that was manually configured. Dynamic : An ARP entry that was learned by the router.





Interface	VLAN 1 V
Interface	Note: Only interfaces with an valid IPv4 address are available for selection
IP Address	192.168.101.100
MAC Address	8C:4D:EA:FE:05:BE

- \geq Interface : Administrator can select VLAN interface.
- \geq **IP Address :** Enter the IPv4 address of add ARP table.
- **MAC Address :** Enter the MAC address of add ARP table.

Configuring a static ARP table can improve communication security. Static ARP Table restricts the use of specified MAC addresses when communicating with devices with specified IP addresses. At this time, the harmful network transmission cannot modify Note the mapping relationship between the IP address and the MAC address of the entry, so as to protect the communication between the device and the specified device.

Click the "Apply" button to save your changes or "Close" the button to close settings.

13.2 IPv6 Management and Interfaces

This chapter describes how to configure the IP interface for management access Switch over the network. The switch supports IP version 4 and version 6,

And can be managed simultaneously by any of these address types. You can manually configure specific IPv4 or IPv6 addresses, or instruct the switch to obtain an IPv4 address from a BOOTP or DHCP server. An IPv6 address can only be configured manually.

IPv6 Configuration – Set the IPv6 address for management access.

13.2.1 **IPv6** Interface

Administrator can configure this "IPv6 Interface Table "page setting for "add" and "Edit" and "Delete" function management.



USER MANUAL



IP Configuration → IPv6 M	anager	nent and	Routing	Þ IPv6 Int	erface		
✤ Status							
		IPv6 Unicas	t Pouting	Enable			
≉ Port	IPv6 Unicast Routing C Enable						
✤ POE Setting	Apply Cancel						
* VLAN		<u>++)</u>		,			
MAC Address Table							
	IPv6 Interface Table						
* Discovery						0 5	
* DHCP	_					ч <u></u>	
✤ Multicast				DHCPv6	Client		
- IP Configuration		Interface	Stateless	Information	Minimum Information	Auto Configuration	DAD Attempts
IPv4 Management and Routing			Juneess	Refresh Time	Refresh Time		
		VLAN 1	Disabled	86400	600	Enabled	1
IPv6 Interface IPv6 Addresses		Add][Edit	Delete]		

IPv6 Unicast Routing : Administrator can configure "Enable" this IPv6 Unicast Routing function.

Note	Next to IPv6 Unicast Routing, specify whether IPv6 unicast routing is globally	
Note	enabled by selecting the Enable radio button or the Disable radio button.	

Click the "Apply" button to save your changes or "*Cancel*" the button to cancel settings.

Select the type of the IPv6 interface through which the IPv6 packets are forwarded. The Switch supports the VLAN interface type and Loopback interface type .

Configuration" Interface" setting on "VLAN" :

Interface	◉ VLAN 1∨	
interiace	Loopback	
Auto Configuration	Enable	
DAD Attempts	1	(0 - 600, default 1)
HCPv6 Client		
Stateless	Enable	
Information Refresh Time	86400	(86400 - 4294967294, default 86400)
Minimum Information Refresh Time	600	(600 - 4294967294, default 600)





- \succ Auto Configuration : The IPv6 address autoconfiguration automatically creates new IPv6 interfaces for a given line description, and assigns IPv6 addresses for the interfaces.
- \geq **DAD Attempts :** Configures the number of neighbor solicitations to be sent when performing duplicate address detection (DAD) for a unicast address configured on an interface. The no form of this command sets the number of attempts to the default value.

DHCP6 Client :

- \geq Stateless : IPv6 stateLess AddressAutoConfiguration(SLAAC) function
- \geq Information Refresh Time : 86400 by default
- \geq Minimum Information Refresh Time : 600 by default

Click the "Apply" button to save your changes or "Close" the button to close settings.

Configuration" Interface" setting on "Loopback" :

Interface	● VLAN 1 ✔
Interlace	🔿 Loopback
Auto Configuration	Enable
DAD Attempts	1 (0 - 600, default 1)
DHCPv6 Client	
Stateless	🗌 Enable
Information Refresh Time	86400 (86400 - 4294967294, default 86400
Minimum Information Refresh Time	600 (600 - 4294967294, default 600)

Loopback : The loopback address may be used by a node to send an IPv6 packet to itself. It must not be assigned to a physical or virtual interface.

Click the "Apply" button to save your changes or "Close" the button to close settings.





IPv6 Addresses 13.2.2

Administrator can configure this "IPv6 Address Table "page setting for "add" and "Delete" function management.

IP Configuration 🏓 IPv6 Ma	nagem	ent and Routin	ig 🖻 IPv6 Addresses	5	
	IPv6 A	ddress Table			
✤ POE Setting	Interfac	e VLAN 1 🗸			
* VLAN					0
♦ MAC Address Table	-				4
		Pv6 Address Type	IPv6 Address	IPv6 Prefix Length	DAD Status
* Discovery		ink Local	fe80::8e4d:eaff:fe30:dd53	64	Active
* DHCP		lulticast	ff02::1:ff30:dd53		
✤ Multicast		lulticast	ff02::1		
- IP Configuration		lulticast	ff01::1		
 IPv4 Management and Routing IPv6 Management and Routing IPv6 Interface IPv6 Addresses 	Ac	ld Delete			

IPv6 Address Table

 \triangleright Interface : From the Interface menu, Administrator can select the VLAN for the IPv6 Interface Selection page displays. The page also shows the IPv6 Interface Configuration table.

Field	Description			
IPv6 Address Type	The IP Prefix for the destination			
IPv6 Address	The prefix length for the active route.			
IPv6 Prefix Length	The type of route: Static or Dynamic, depending on how the route was added.			
DAD status	 Shows the state of the IPv6 address. The state can be one of the following Tent : Routing is disabled or the address does not work because of a "duplicate address detection" (DAD) condition. Active : The IPv6 address is valid and active. Preferred : The IPv6 address was verified to be unique, valid, and active. 			





Select the type of the IPv6 Address through which the IPv6 format are use. The Switch supports the Global type and Link Local type . *Configuration" IPv6 Address Type" setting on "Global " :*

Interface	VLAN 1
IPv6 Address Type	● Global ○ Link Local
IPv6 Address	fe80::8e4d:eaff:fe30:dd55
Prefix Length	32 (3 - 128)
EUI-64	Enable

- > IPv6 Address Type :
- **Global :** Configures an IPv6 global unicast address with a full IPv6 address including the network prefix and host address bits, followed by a forward slash, and a decimal value indicating how many contiguous bits of the address comprise the prefix.
- Link Local : Configures an IPv6 link-local address. The address prefix must be in the range of FE80 to FEBF. and you can configure only one link-local address per interface.(The specified address replaces a link-local address that was automatically generated for the interface).
- IPv6 Address : Full in your IPv6 address . Example of IPv6 input network range: 2001: 8E4D: EAFF: FE01: 0000: 0000: 0000: 0002 ~ FFFF: FFFF: FFFF: FFFE. (For IPv6 IP acquisition, May please contact your ISP provider).
- > **Prefix Length :** The Prefix Length of the IPv6 address of the Switch .
- EUI-64 : Use this section to tick the Enable for EUI-64 format IPv6 configuration, Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.

The switch must be configured with a link-local address. Therefore, any configuration process that enables IPv6 functionality, including address auto configuration, explicitly enabling IPv6 or manually assigning a global unicast address will also automatically generate a link-local unicast address. The prefix length for a link local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier.





Click the "Apply" button to save your changes or "Close" the button to close settings.

Interface	VLAN 1
IPv6 Address Type	 ○ Global ● Link Local
IPv6 Address	FE80::8E4D:EAFF:FE05:3406
	(3 - 128)
	🗌 Enable

Configuration" IPv6 Address Type" setting on "Link Local" :

IPv6 Addrress : This section uses the Link Local address of the local identifier interface required by the IPv6 mode address operation specification, for example, it is as "FE80::8E4D:EAFF:FE05:3406".

Click the "Apply" button to save your changes or "Close" the button to close settings.

13.2.3 IPv6 Routers

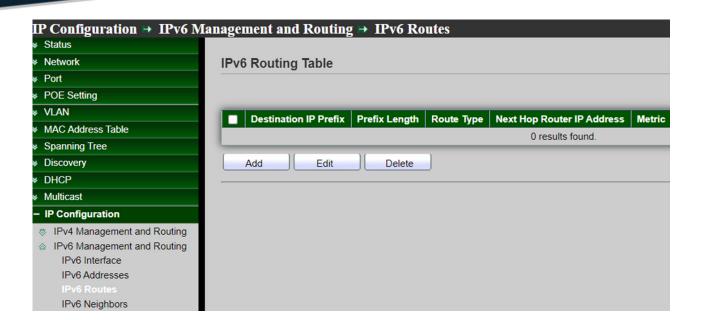
You can enter static routes in the routing table using the IP > Static Routes (Add) page. Static routes may be required to force the use of a specific route to a subnet. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network

This page system can displayed IPv6 Routing Table for "Destination IP Prefix" / Prefix Length / Route Type / Next Hop Router IP Address / Metric / Administrative Distance / Outgoing Interface information.

Administrator can configure this "IPv6 Routing Table" page setting for **"add"** and "Edit" and **"Delete"** function management.



USER MANUAL



IPv6 Routing Table						
					Q _	
Destination IP Prefix	Prefix Length	Route Type	Next Hop Router IP Address	Metric	Administrative Distance	Outgoing Interface
			0 results found.			

Field	Description
Destination IP Prefix	The IP Prefix for the destination
Prefix Length	The prefix length for the active route.
	The type of protocol for the active route:
	Static. The route was manually defined.
Router Type	• ND (Neighbor Discovery). The route was discovered through the ND protocol.
	 Connected. The route was derived from a manually configured IPv6 address.
Next Hop Router IP Address	The next hop IPv6 address for the active route.
Metric	The Metric value for the configured next hop.





Specify the Metric (sometimes called administrative dista	
	is an integer value from 1 to 255.
Administrative Distance	The route administrative distance of the configured route.
Outgoing Interface	The outgoing interface of the route active or inactive.

IPv6 Prefix			
IPv6 Prefix Length		(0 - 128)	
Next Hop Router IP Address			
Metric	1	(1 - 255, default 1)	

- \succ IPv6 Prefix : In the IPv6 Prefix field, specify the IPv6 network prefix for the destination..
- \geq IPv6 Prefix Length : In the IPv6 Prefix Length field, specify the IPv6 prefix length for the destination..
- **Next Hop Router IP Address :** In the Next Hop IPv6 Address field, specify the outgoing \geq router IPv6 address to use when forwarding traffic to the next router (if any) in the path toward the destination.

Note	9	The next router is always one of the adjacent neighbors or the IPv6 address of the local interface for a directly attached network.		
		ric : Please fill in the cost (hop count) of transmission you want to apply for routing		
	purp	ooses.		
Note	9	This metric represents the "cost" of transmission for routing purposes. IP routing uses "hop count" as a measure of cost, with a minimum value of 1 for directly connected networks. Enter a number that approximates the cost of this link. The		

or 3 is usually suggested here to fill in the frequently used numbers.

Click the "Apply" button to save your changes or "Close" the button to close settings.







IPv6 Neighbors 13.2.4

Administrator can configure this "IPv6 Neighbor Table "page setting for "add" and "Edit" and "Delete" function management.

IP Configuration 😐 IPv6 M	anagement and Routing \mapsto IPv6 Neighbors
	O All
✤ Port	Clear Neighbor Table
✤ POE Setting	⊖ Static
* VLAN	N/A
MAC Address Table	Apply Cancel
* Discovery	
* DHCP	IPv6 Neighbor Table
✤ Multicast	
- IP Configuration	Q
 IPv4 Management and Routing IPv6 Management and Routing 	■ Interface IPv6 Address MAC Address Status Router
 IPv6 Management and Routing IPv6 Interface 	0 results found.
IPv6 Addresses	Add Edit Delete
IPv6 Routes	Add Edit Delete
IPv6 Neighbors	
	namic Itic A
Apply Cancel	
IPv6 Neighbor Table	
	Q 8c
Interface IPv6 Addres	s MAC Address Status Router
VLAN 1 fe80::8e4d:eaaa:fe	05:3408 8c:4d:ea:fe:05:be Static N/A
VLAN 1 fe80::8e4d:eaff:ee0	9:3589 8c:4d:ea:fe:cc:ee Static N/A
VLAN 1 fe80::8e4d:eaff:fe0	5:3406 8c:4d:ea:fe:05:06 Static N/A
Add Edit	

Clear Neighbor Table

The administrator can select the filter Status type including by "All" or "Dynamic" or "Static" or "N/A "to quickly select batches to clear the "IPv6 Neighbor Table".





Use the "Search" menu to consult the list.

Search by "Keyword" using the Search menu and field. For example, '8c'. Then click the Search icon button. If the address exists, show the entry.

Field	Description	
	The interface whose settings are displayed in the current table row.	
Interface	This field displays the ID number of the IPv6 interface on which the IPv6	
	address is created or through which the neighboring device can be reached.	
IPv6 Address	The IPv6 address of the neighbor or interface.	
	This field displays the MAC address of the IPv6 interface on which the IPv6	
MAC Address	address is configure or the MAC address of the neighboring device.	
Status	The state of the neighbor cache entry. The states for "dynamic entries" or "Static entries"in the IPv6 neighbor discovery cach.	
Router	Neighbor for the active route.	

Add Neighbor	
Interface	VLAN 1 V
IP Address	
MAC Address	
Apply C	lose

- > Interface : Select the type of IPv6 interface for VLAN ID configure.
- \geq IP Addrress : Specify the IPv6 address of the neighboring device which can be reached through the interface.
- MAC Addrerss : Specify the MAC address of the neighboring device which can be reached \succ through the interface.

Click the "Apply" button to save your changes or "Close" the button to close settings.





14. Security

14.1 RADIUS

Network architecture can establish a Remote Authorization login Service (RADIUS) server to provide a centralized 802.1X or MAC-based network access control for all of its devices. This switch can act as a RADIUS client that uses the RADIUS server to provide centralized security and authorization and user authentication.

Administrator can set account for the switch on the RADIUS server, and configure that RADIUS server along with the other parameters on the RADIUS page.

Security > RADIUS								
✤ Network	Use Default Paran	neter						
✤ Port				1 10 de	foult 2)			
✤ POE Setting	Retry 3		((1 - 10, d€	ault 3)			
* VLAN	Timeout 3		5	Sec (1 - 3	0, default 3)			
 MAC Address Table 								
 Spanning Tree 	Key String							
* Discovery			_		_		-	
* DHCP	Apply							
✤ Multicast	RADIUS Table							
 IP Configuration 								
– Security	Showing All 🗸 entrie	S	Showing	g 1 to 1 o	f 1 entries		(Q
RADIUS	Server Address	Server Port	Priority	Retry	Timeout	Usage		
TACACS+	192,168,2,99	1812	1	3	3	All		
AAA	102.100.2.33	1012		3	5	7.01	First	Draviaus
 Management Access Authentication Manager 	Add	dit Del	lete				First	Previous

Use Default Parameters :

- **Retry:** Set default retry number ,Enter the number of transmitted requests that are sent to the RADIUS server before a failure is considered to have occurred. Default is 3.
- **Timeout:** Set default timeout value ,Enter the number of seconds that the switch waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Default is 3.
- **Key String:** Set default RADIUS key string ,The key string used security communications between the switch and the RADIUS server by MD5.This key must match the key configured on the RADIUS server. If don't have an encrypted key string (from other device), please enter the key string in plaintext form.

Click the "Apply" button to save your changes settings.





Field	Description	
Server Address	RADIUS server address.	
Server Port	RADIUS server port.	
	RADIUS server priority (smaller value has higher priority). RADIUS	
	session will try to establish with the server setting which has highest	
Priority	priority. If failed, it will try to connect to the server with next higher	
	priority.	
Retry	RADIUS server retry value. If it is fail to connect to server, it will keep trying until timeout with retry times.	
	RADIUS server timeout value. If it is fail to connect to server, it will	
Timeout	keep trying until timeout.	
	RADIUS server usage type	
	Login: For login authentication.	
Usage	• 802.1x: For 802.1x authentication.	
	All: For alltypes.	

Address Type	 Hostname IPv4 IPv6 	
Server Address	192.168.2.99	
Server Port	1812	(0 - 65535, default 1812)
Priority	1	(0 - 65535)
Key String	✔ Use Default	
Retry	Use Default	(1 - 10, default 3)
Timeout	Use Default	Sec (1 - 30, default 3)
Usage	 Login 802.1X All 	



- \geq Address Type: Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type
 - Hostname: Use domain name as server address.
 - **IPv4:** Use IPv4 as server address.
 - **IPv6:** Use IPv6 as server address.
- Server Address: Please enter the IP address or hostname of the RADIUS server. In add dialog, \geq user need to input server address based on address type. In edit dialog, it shows current edit server address.
- Server Port: Set port of RADIUS server. \geq
- \geq **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set RADIUS server priority (smaller value has higher priority). RADIUS session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- \succ **Key String:** Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the RADIUS server. This key must match the key configured on the RADIUS server. If administrator select use default (checked in checkbox) will use the default key string.
- **Retry:** Select User Defined to enter the number of requests that are sent to the RADIUS server \geq before a failure is considered to have occurred, or select Use Default to use the default value.
- Timeout: Select User Defined to enter the number of seconds that the switch waits for an \geq answer from the RADIUS server before retrying the query or switching to the next server, or select Use Default to use the default value. Set RADIUS server timeout value. If it is fail to connect to server, it will keep trying until timeout.
- \geq **Usage:** Select the RADIUS server authentication type.
 - Login: RADIUS server is used for authenticating users that want to administer the switch.
 - **802.1X:** RADIUS server is used for authentication in 802.1X access control.
 - All: RADIUS server is used for authenticating user that wants to administer the switch and for authentication in 802.1X access control.

Click the "Apply" button to save your changes or "Close" the button to close settings.





14.2 TACACS+

Administrator can be configuration TACACS+ to connection TACACS+ Server to provide authentication and authorization for all devices in the organization.

This page allow user to add, edit or delete TACACS+ server settings and modify default parameter of TACACS+ server.

Security → TACACS+	
* Network	Use Default Parameter
✤ Port	
POE Setting	Timeout 5 Sec (1 - 30, default 5)
* VLAN	Key String
MAC Address Table	
 Spanning Tree 	Apply
* Discovery	
* DHCP	TACACS+ Table
 Multicast 	
* IP Configuration	Showing All v entries Showing 1 to 1 of 1 entries
– Security	
RADIUS	Server Address Server Port Priority Timeout
TACACS+	192.168.2.101 49 2 5
AAA	First
Management Access	Add Edit Delete

> Use Default Parameters :

- **Timeout:** Enter the amount of time in seconds that passes before the connection between the switch and the TACACS+ server times out. If a value is not entered for an individual server, the value is taken from this field, default is 5.
- **Key String:** Enter the default key string in encrypted or plaintext form used for communicating with all TACACS+ servers.

Note If administrator don't enter the default key string here, the key entered on the Add page must match the encryption key used by the TACACS+ server or enter the default key string here and a key string for an individual TACACS+ server, the key string configured for the individual TACACS+ server takes precedence.

Click the "Apply" button to save your changes settings.





Field	Description		
Server Address	TACACS+ server address.		
Server Port	TACACS+ server port.		
	TACACS+ server priority (smaller value has higher priority).		
	TACACS+ session will try to establish with the server setting which		
Priority	has highest priority. If failed, it will try to connect to the server		
	with next higher priority.		
	RADIUS server retry value. If it is fail to connect to server, it will		
Retry	keep trying until timeout with retry times.		
T	TACACS+ server timeout value. If it is fail to connect to server, it		
Timeout	will keep trying until timeout.		

Address Type	 Hostname IPv4 IPv6 	
Server Address	192.168.2.101	
Server Port	49	(0 - 65535, default 49)
Priority	2	(0 - 65535)
Key String	✓ Use Default	
Timeout	✓ Use Default 5	Sec (1 - 30, default 5)

 \succ Address Type: Select IP Version 4 / 6 or use Hostname typem, In add dialog, user need to specify server Address Type

- Hostname: Use domain name as server address.
- IPv4: Use IPv4 as server address.
- **IPv6:** Use IPv6 as server address.
- \succ Server Address: In add dialog, user need to input server address based on address type. In edit





dialog, it shows current edit server address.

- Server Port: Set TACACS+ server port. \geq
- \geq **Priority:** Administrator can enter the priority of the server. The priority determines the order that the switch attempts to contact the servers to authenticate users. The switch first starts with the highest priority server. 0 is the high priority, Set TACACS+ server priority (smaller value has higher priority). TACACS+ session will try to establish with the server setting which has highest priority. If failed, it will try to connect to the server with next higher priority.
- \geq Key String: Administrator can select user defined Encrypted or Plaintext to enter the key string form used for authenticating and encrypting the communication between the switch and the TACACS+ server. This key must match the key configured on the TACACS+ server. If administrator select use default (checked in checkbox) will use the default key string.
- Timeout: Set TACACS+ server timeout value. If it is fail to connect to server, it will keep trying \geq until timeout.

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.3 AAA

14.3.1 Method List

Administrator can set groups of AAA security, each group have 4 method table, each method can select 1 of 6 type which contains Empty / None / Local / Enable / RADIUS and TACACS+. This page allow user to add, edit or delete login authentication list settings (The "default" list cannot be deleted.). The line combined to this list will authenticate login user by methods in this list. If the first method is failed, it will try to use the next priority method to authenticate if it exists.With RADIUS and TACACS+ methods, the failed means connecting to server fail. With Local method, the failed means cannot find the user in local database.



USER MANUAL



Security → AAA → Method	List
* Network	Method List Table
* Port	
POE Setting	Showing All v entries Showing 1 to 1 of 1 entries Q
* VLAN	Name Sequence
MAC Address Table	
 Spanning Tree 	default (1) Local
* Discovery	First Previ
* DHCP	Add Edit Delete
* Multicast	
IP Configuration	
– Security	
RADIUS	
TACACS+	
AAA	
Method List	
Login Authentication	
Management Access	
 Authentication Manager 	
Port Security	
Protected Port	
Storm Control	
© DoS	
 Dynamic ARP Inspection 	
DHCP Snooping	
IP Source Guard	

Field	Description
	Login authentication list name. This name should be different from
Name	other existing lists.
	Priority of login authentication method.
	 None: Authenticated with any condition.
-	 Local: Use local accounts database to authenticate
Sequence	 TACACS+: Use remote TACACS+ server to authenticate.
	RADIUS: Use remote Radius server to authenticate.
	Enable: Use local enable password to authenticate



Edit Method Li	st
Name	default
Method 1	Empty None Local Enable RADIUS TACACS+
Method 2	Empty None Local Enable RADIUS TACACS+
Method 3	Empty None Local Enable RADIUS TACACS+
Method 4	Empty None Local Enable RADIUS TACACS+
Apply	Close

- \geq Name: Login authentication list name. This name should be different from other existing lists.
- \succ Method 1: Select first priority of login authentication method.
 - None: Authenticated with any condition.
 - Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
 - **RADIUS:** Use remote Radius server to authenticate.
 - Enable: Use local enable password to authenticate.
- \geq Method 2: Select first priority of login authentication method.
 - None: Authenticated with any condition.
 - Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
 - **RADIUS:** Use remote Radius server to authenticate.
 - Enable: Use local enable password to authenticate.
- \geq **Method 3:** Select first priority of login authentication method.
 - None: Authenticated with any condition.
 - Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
 - **RADIUS:** Use remote Radius server to authenticate.
 - Enable: Use local enable password to authenticate.
- Method 4: Select first priority of login authentication method. \geq



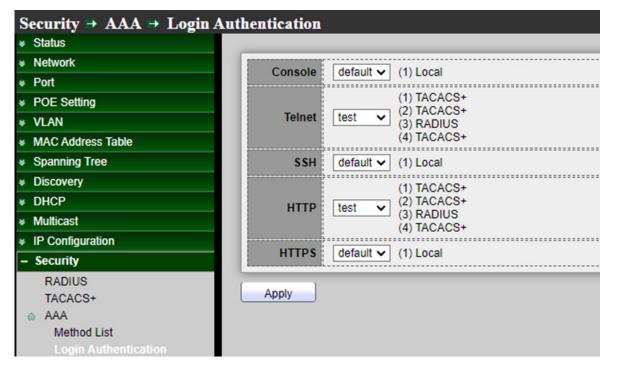


- None: Authenticated with any condition.
- Local: Use local accounts database to authenticate TACACS+: Use remote TACACS+ server to authenticate.
- **RADIUS:** Use remote Radius server to authenticate.
- Enable: Use local enable password to authenticate.

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.3.2 **Login Authentication**

When administrator has created security groups in "AAA → method" then administrator can select different security group in service port.



Field	Description
Console	Specify login authentication list combined on console
Telnet	Specify login authentication list combined on Telnet
SSH	Specify login authentication list combined on SSH
HTTPS	Specify login authentication list combined on HTTPS

Click the "Apply" button to save your changes settings.



14.4 Management Access

14.4.1 Management Service

Administrator can select enable Telnet / SSH / HTTP / HTTPS / SNMP by different protocol to login service and configuration login timeout limit and password error retry count limit.

Status		
Network	Managemen	nt Service
Port	Telnet	Enable
POE Setting	SSH	
VLAN	НТТР	Z Enable
MAC Address Table		
Spanning Tree	HTTPS	_
Discovery	SNMP	
DHCP	Session Tim	neout
Multicast		
IP Configuration	Console	10 Min (0 - 65535, default 10)
Security	Telnet	10 Min (0 - 65535, default 10)
RADIUS	SSH	10 Min (0 - 65535, default 10)
TACACS+	3311	
Management Access	нттр	10 Min (0 - 65535, default 10)
	HTTPS	10 Min (0 - 65535, default 10)
Management ACL		
Management ACE Authentication Manager	Password R	Retry Count
Port Security	Console	3 (0 - 120, default 3)
Protected Port		
Storm Control	Telnet	3 (0 - 120, default 3)
DoS	SSH	3 (0 - 120, default 3)
Dynamic ARP Inspection DHCP Snooping		
IP Source Guard	Silent Time	
ACL	Console	0 Sec (0 - 65535, default 0)
QoS		
Diagnostics	Telnet	0 Sec (0 - 65535, default 0)
Management	SSH	0 Sec (0 - 65535, default 0)

> Management Service: Management service admin state.

- **Telnet:** Connect CLI through telnet.
- SSH: Connect CLI through SSH.
- **HTTP:** Connect WEBUI through HTTP.
- **HTTPS:** Connect WEBUI through HTTPS.
- **SNMP:** Manage switch trough SNMP.

Session Timeout: Set session timeout minutes for user access to user interface. 0 minutes means never timeout, After login management page, in the set time if not session then system will auto timeout, administrator need re-login.

- **Console:** Set console for session timeout 0~65535 minutes.
- **Telnet:** Set Telnet for session timeout 0~65535 minutes.

V1.0a

+(886) 2-8911-6160



USER MANUAL



- SSH: Set SSH for session timeout 0~65535 minutes.
- HTTP: Set HTTP for session timeout 0~65535 minutes.
- HTTPS: Set HTTPS for session timeout 0~65535 minutes.
- \geq Password Retry Count: Retry count is the number which CLI password input error tolerance count. After input error password exceeds this count, the CLI will freeze after silent time, If login error reaches the set value then login page will be kicked out, administrator need reopen the login page.
 - Console: Set console for password Retry count of 0~120.
 - **Telnet:** Set Telnet for password Retry count of 0~120.
 - SSH: Set SSH for password Retry count of 0~120.
- \geq Silent Time: This function to be matched "Password Retry Count" function, if login error reaches the set value within then set value of silent time will can't be reopen login page until the set time end ,After input error password exceeds password retry count, the CLI will freeze after silent time.
 - Console: Set console for Silent Time of 0~65535 minutes.
 - Telnet: Set Telnet for Silent Time of 0~65535 minutes.
 - SSH: Set SSH for for Silent Time of 0~65535 minutes .

14.4.2 Management ACL

Administrator can create ACL and set Active or Deactive the rules.

If administrator set "Active" will be apply "Management ACE" rules. ACL can set which ports is Permit or Deny connection to which services of the switch management interface.

If only create one ACL Profile and click Active then these all ports and services Note will are all denied.



USER MANUAL



Security 🖻 Management Ac	cess ⇒ Management ACL
Network	
✤ Port	ACL Name
POE Setting	
* VLAN	Apply
MAC Address Table	
Spanning Tree	Management ACL Table
Solution State	
* DHCP	Showing All entries Showing 1 to 1 of 1 entries Q
 Multicast 	ACL Name State Rule
IP Configuration	ACL Hame State Rule
– Security	First Previo
RADIUS TACACS+ AAA Management Access Management Access Management ACL Management ACL Management ACE Authentication Manager Port Security Protected Port Storm Control DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard	Active Deactive Delete

\succ ACL Name: Input MAC ACL name.

Click the "Apply" button to save your changes settings.

Field	Description
ACL Name	Display Management ACL name
State	Display Management ACL whether active.
Rule	Display the number Management ACE rule of ACL

Set the "Active" and "Deactive" and "Delete" for this table management.





14.4.3 **Management ACE**

This management ACE page is to create an ACL profile rule. Administrator can select an created ACL profile to set security rule. If set the ACE only use Telnet a single rule. After confirmation the rule will apply to ACL profile.

Administrator can go to "management ACL" page click "Active" button to enable the rule. After active the rule, this management page will can't operating only use Telnet protocol to management, Setting "add" and "Edit" and "Delete" function for this management.

Security → Management Ac	cess ⇒ M	anagement	ACE		
✓ Network					
✤ Port	ACL Name	e test1 🗸			
 POE Setting 	ACL Name	e lesti 🗸			
* VLAN	Showing	All 🗸 entries	Sh	owing 1 to 1	of 1 entries Q
MAC Address Table					
 Spanning Tree 	Pri Pri	ority Action	Service	Port	Address / Mask
* Discovery		1 Deny	Snmp	GE2-GE3	192.168.2.77 / 255.255.255.0
* DHCP					First Previous 1
 Multicast 	Add	Edit		Delete	
IP Configuration					
– Security					
RADIUS					
TACACS+					
⊗ AAA					
 Management Access Management Service 					
Management ACL					
Management ACE					

ACL Name: Select the ACL name to which an ACE is being added. \geq

Field	Description
Priority	Display the priority of ACE.
Action	Display the action of ACE
Service	Display the service ACE.
Port	Display the port list of ACE.
Address / Mask	Display the source IP address and mask of ACE.







ACL Name	test1			
Priority	1 (1 - 655			
Service	 All Http Https Snmp SSH Telnet 			
Action	 Permit Deny 			
Port	GE6 GE7	Selected Por GE3 GE2	t ,	
IP Version	 All IPv4 IPv6 			
IPv4	192.168.2.77		/ 255.255.255.0]
IPv6			/ 128	 (1 - 128

- > ACL Name: Display the ACL name to which an ACE is being added.
- Priority: Set this rule priority, Specify the priority of the ACE. ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- Service: Select the type service of rule.
 - All: All services .
 - **HTTP**: Only HTTP service .
 - **HTTPs**: Only HTTPs service.
 - **SNMP**: Only SNMP service.
 - **SSH:** Only SSH service.
 - Telnet: Only Telnet service
- Action: Select the action after ACE match packet.
 - **Permit**: Forward packets that meet the ACE criteria.
 - **Deny**: Drop packets that meet the ACE criteria.

+(886) 2-8911-6160





- \geq Port: Select ports which will be matched.
- \geq **IP Version:** Select the type of source IP address.
 - All: All IP addresses can access.
 - IPv4: Specify IPv4 address ca access.
 - IPv6: Specify IPv6 address ca access
- \geq **IPv4:** Enter the source IPv4 address value and mask to which will be matched.
- **IPv6:** Enter the source IPv6 address value and mask to which will be matched. \geq

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.5 Authentication Manager

14.5.1 Property

This page allow user to edit authentication global settings and some port mods' configurations, Administrator can edit authentication global settings and some port mods' configurations.

Status												
Network	-				2 902 1v					1		
Port					✓ 802.1x							
POE Setting		Authentication Type				MAC-Based WEB-Based						
VLAN												
MAC Address Table												
Spanning Tree				Guest VLAN	1.							
Discovery										4		
онср		MAC-B	ased Use	er ID Forma		XXXXX 🗸				1		
Multicast	-											
P Configuration	A	Apply	J									
Security												
RADIUS	Port	Mode	Table									
TACACS+												
										~ ~		
AAA										0		
	-									Q [
Management Access		Entry	Port		uthentication		Host Mode	Order	Method		VLAN Assign Mo	
Management Access Authentication Manager Property		Entry	Port	م 802.1x	uthentication 1 MAC-Based	Type WEB-Based	Host Mode	Order	Method	Q Guest VLAN	VLAN Assign Mo	
Management Access Authentication Manager Property Port Setting		Entry 1	Port GE1				Host Mode Multiple Authentication	Order 802.1x			VLAN Assign Mo	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account		Entry 1		802.1x	MAC-Based	WEB-Based				Guest VLAN		
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account		1	GE1	802.1x Disabled	MAC-Based Disabled	WEB-Based Disabled	Multiple Authentication	802.1x	RADIUS	Guest VLAN Disabled	Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions		1	GE1 GE2	802.1x Disabled Disabled	MAC-Based Disabled Disabled	WEB-Based Disabled Disabled	Multiple Authentication Multiple Authentication	802.1x 802.1x	RADIUS RADIUS	Guest VLAN Disabled Disabled	Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account		1 2 3	GE1 GE2 GE3	802.1x Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled	Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security		1 2 3 4	GE1 GE2 GE3 GE4 GE5	802.1x Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port		1 2 3 4 5 6	GE1 GE2 GE3 GE4 GE5 GE6	802.1x Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control DoS Dynamic ARP Inspection		1 2 3 4 5 6 7	GE1 GE2 GE3 GE4 GE5 GE6 GE7	802.1x Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control Dos Dynamic ARP Inspection DHCP Snooping		1 2 3 4 5 6 7 8	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8	802.1x Disabled Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static Static	
Management Access Authentication Manager Property MAC-Based Local Account WEB-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard		1 2 3 4 5 6 7 8 9	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9	802.1x Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard CL		1 2 3 4 5 6 7 8 9 10	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9 GE10	802.1x Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static Static Static Static	
Management Access Authentication Manager Property Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control DoS Dynamic ARP Inspection DHCP Snooping IP Source Guard CL		1 2 3 4 5 6 7 8 9	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9	802.1x Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static Static Static	
Port Setting MAC-Based Local Account WEB-Based Local Account Sessions Port Security Protected Port Storm Control DoS Dos		1 2 3 4 5 6 7 8 9 10	GE1 GE2 GE3 GE4 GE5 GE6 GE7 GE8 GE9 GE10	802.1x Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	MAC-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	WEB-Based Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication Multiple Authentication	802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x 802.1x	RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS RADIUS	Guest VLAN Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled Disabled	Static Static Static Static Static Static Static Static Static Static	

Authentication Type : Set checkbox to enable/disable following authentication types \geq

- 802.1x: Use IEEE 802.1x to do authentication
- MAC-Based: Use MAC address to do authentication
- WEB-Based: Prompt authentication web page for user to do authentication





- \geq Guest VLAN : Set checkbox to enable/disable guest VLAN, if guest VLAN is enabled, you need to select one available VLAN ID to be guest VID.
- \geq MAC-Based User ID Format : Select mac-based authentication RADIUS username/password ID format.
 - XXXXXXXXXXXXX
 - XXXXXXXXXXXXX
 - XX:XX:XX:XX:XX:XX
 - XX:XX:XX:XX:XX:XX
 - XX-XX-XX-XX-XX-XX
 - XX-XX-XX-XX-XX-XX
 - XX.XX.XX.XX.XX.XX
 - XX.XX.XX.XX.XX.XX
 - XXXX:XXXX:XXXX
 - XXXX:XXXX:XXXX
 - XXXX-XXXX-XXXX
 - XXXX-XXXX-XXXX
 - XXXX.XXXX.XXXX
 - XXXX.XXXX.XXXX
 - XXXXXX:XXXXXX
 - XXXXXX:XXXXXX
 - XXXXXX-XXXXX
 - XXXXXX-XXXXXX

Click the "Apply" button to save your changes settings.

Port	Mode	Table								
	Entry	Port		Authentication		Host Mode	Order	Method	Guest VLAN	VLAN Assign Mode
	1	GE1	802.1x Enabled	MAC-Based Enabled	WEB-Based Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
	2	GE2	Enabled	Enabled	Enabled	Multiple Authentication	802.1x, WEB-Based	RADIUS , Local	Enabled	Disable
	3	GE3	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
	4	GE4	Enabled	Enabled	Enabled	Multiple Authentication	802.1x , WEB-Based	RADIUS , Local	Enabled	Disable
	5	GE5	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	6	GE6	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	7	GE7	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	8	GE8	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static
	9	GE9	Disabled	Disabled	Disabled	Multiple Authentication	802.1x	RADIUS	Disabled	Static





Field	Description			
Port	Port name			
Authentication Type (802.1X)	 802.1 X authentication type state Enabled: 802.1X is enabled Disabled: 802.1X is disabled 			
Authentication Type (MAC-Based)	 MAC-Based authentication type state Enabled: MAC-Based authentication is enabled Disabled: MAC-Based authentication is disabled 			
Authentication Type (WEB-Based)	 WEB-Based authentication type state Enabled: WEB-Based authentication is enabled Disabled: WEB-Based authentication is disabled 			
Host Mode	 Authenticating host mode Multiple Authentication: In this mode, every client need to pass authenticate procedure individually. Multiple Hosts: In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode. Single Host: In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1. 			
Order	Support following authentication type order combinations. We Authentication should always be the last type. The authenticati manager will go to next type if current type is not enabled or authenticated fail. • 802.1x • MAC-Based • WEB-Based • 802.1x MAC-Based • 802.1x WEB-Based • MAC-Based 802.1x • WEB-Based 802.1x • WEB-Based 802.1x • 802.1x MAC-Based WEB-Based • 802.1x WEB-Based WEB-Based			





	Support following authentication method order combinations.					
	These orders only available on MAC-Based authentication and					
	WEB-Based authentication. 802.1x only support Radius method.					
Method	 Local: Use DUT's local database to do authentication 					
	 Radius: Use remote RADIUS server to do authentication 					
	Local Radius					
	RadiusLocal					
	Port guest VLAN enable state					
Guest VLAN	 Enabled: Guest VLAN is enabled on port 					
	Disabled: Guest VLAN is disabled on port					
	Support following VLAN assign mode and only apply when source					
	is					
	RADIUS					
	 Disable: Ignore the VLAN authorization result and keep 					
	original VLAN of host.					
VLAN Assign Mode	 Reject: If get VLAN authorized information, just use it. 					
	However, if there is no VLAN authorized information, reject					
	the host and make it unauthorized.					
	• Static: If get VLAN authorized information, just use it. If					
	there is no VLAN authorized information, keep original VLAN					
	of host.					





Port							
	✓ 802.1x						
Authentication Type	MAC-Based						
	WEB-Based						
	Multiple Authentication						
Host Mode							
	◯ Single Host						
	Available Type Select Type						
Order	MAC-Based Block Based WEB-Based						
	Available Method Select Method						
	Local A RADIUS A						
Method							
							
Guest VLAN	Enable						
	O Disable						
VLAN Assign Mode	⊖ Reject						
	Static						

- **Port :** Display selected Port number.
- > Authentication Type : Set checkbox to enable/disable authentication types.
 - 802.1x : Use IEEE 802.1x to do authentication
 - MAC-Based : Use MAC address to do authentication
 - WEB-Based : Prompt authentication web page for user to do authentication
- **Host Mode :** Select authenticating host mode.
 - **Multiple Authentication :** In this mode, every client need to pass authenticate procedure individually
 - Multiple Hosts : In this mode, only one client need to be authenticated and other clients will get the same access accessibility. Web-auth cannot be enabled in this mode.
 - **Single Host :** In this mode, only one host is allowed to be authenticated. It is the same as Multi-auth mode with max hosts number configure to be 1.
- Order : Support following authentication type order combinations. Web Authentication should always be the last type. The authentication manager will go to next type if current





type is not enabled or authenticated fail.

- 802.1x
- MAC-Based
- WEB-Based
- 802.1x MAC-Based
- 802.1x WEB-Based
- MAC-Based 802.1x
- WEB-Based 802.1x
- 802.1x MAC-Based WEB-Based
- 802.1x WEB-Based MAC-Based
- Method : Support following authentication method order combinations. These orders only available on MAC-Based authentication and WEB-Based authentication. 802.1x only support Radius method.
 - Local : Use DUT's local database to do authentication
 - Radius : Use remote RADIUS server to do authentication
- **Guest VLAN :** Set checkbox to enable/disable guest VLAN.
- VLAN Assign Mode : Support following VLAN assign mode and only apply when source is RADIUS.
 - **Disable**: Ignore the VLAN authorization result and keep original VLAN of host.
 - **Reject**: If get VLAN authorized information, just use it. However, if there is no VLAN authorized information, reject the host and make it unauthorized.Local Radius.
 - **Static**: If get VLAN authorized information, just use it. If there is no VLAN authorized information, keep original VLAN of host.

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.5.2 Port Setting

Administrator can configure authentication manger port settings, This page allow user to configure authentication manger port settings





Security > Authentication	Manag	er 🔁]	Port S	etting					
* Network	Por	t Settin	g Tabl	е					
* Port	-								
* POE Setting									
* VLAN							Commo	n Timer	
 MAC Address Table 		Entry	Port	Port Control	Reauthentication	Max Hosts	Reauthentication	Inactive	Quiet
 Spanning Tree 		1	GE1	Auto	Enabled	256	3600	60	60
* Discovery		2	GE2	Auto	Enabled	256	3600	60	60
* DHCP									
 Multicast 		3	GE3	Auto	Enabled	256	3600	60	60
IP Configuration		4	GE4	Disabled	Disabled	256	3600	60	60
– Security		5	GE5	Disabled	Disabled	256	3600	60	60
RADIUS		6	GE6	Disabled	Disabled	256	3600	60	60
TACACS+		7	GE7	Disabled	Disabled	256	3600	60	60
AAA		8	GE8	Disabled	Disabled	256	3600	60	60
Management Access		9	GE9	Disabled	Disabled	256	3600	60	60
Authentication Manager		10	GE10	Disabled	Disabled	256	3600	60	60
Property Port Setting		11	GE11	Disabled	Disabled	256	3600	60	60

Port Setting Table

_	Entry	Port	Port Control	Reauthentication		Commo	n Timer			802.1x Pa	rameters		Web-Based Parameters
	Enuy	POIL	Port Control	Reaumentication	Max Hosts	Reauthentication	Inactive	Quiet	TX Period	Supplicant Timeout	Server Timeout	Max Request	Max Login
	1	GE1	Auto	Enabled	256	3600	60	60	30	30	30	2	3
	2	GE2	Auto	Enabled	256	3600	60	60	30	30	30	2	3
	3	GE3	Auto	Enabled	256	3600	60	60	30	30	30	2	3
	4	GE4	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	5	GE5	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	6	GE6	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	7	GE7	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	8	GE8	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	9	GE9	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
			Disabled	Disabled		3600							
	11	GE11	Disabled	Disabled	256	3600	60	60	30	30	30	2	3
	12	GE12	Disabled	Disabled	256	3600	60	60	30	30	30	2	3

Field	Description
Port	Port name
	Support following authentication port control types.
	 Disable: Disable authentication function and all clients have
	network accessibility.
	 Force Authorized: Port is force authorized and all clients have
Port Control	network accessibility.
	 Force Unauthorized: Port is force unauthorized and all clients
	have no network accessibility.
	 Auto: Need passing authentication procedure to get network accessibility.





	Reautheticate state
	 Enabled: Host will be reauthenticated after reauthentication
Reauthentication	period
	• Disabled: Host will not be reauthenticated after reauthentication
	period.
Max Hosts	In Multiple Authentication mode, total host number cannot not exceed max hosts number
	Reauthentication: After re-authenticate period, host will return to
	initial state and need to pass authentication procedure again.
	 Inactive: If no packet from the authenticated host, the inactive
	timer will increase. After inactive timeout, the host will be
	unauthorized and corresponding session will be deleted. In
Common Timer	multi-host mode, the packet is counting on the authorized host
	only and not all packets on the port.
	Quiet: When port is in Locked state after authenticating fail
	several times, the host will be locked in quiet period. After this
	quiet period, the host is allowed to authenticate again.
	• TX Period: Number of seconds that the device waits for a response
	to an Extensible Authentication Protocol (EAP) request/identity
	frame from the supplicant (client) before resending the request.
	 Supplicant Timeout: The maximum number of EAP requests that
	can be sent. If a response is not received after the defined period
802.1X Params	(supplicant timeout), the authentication process is restarted.
	 Server Timeout: Number of seconds that lapses before EAP
	requests are resent to the supplicant.
	Max Request: Number of seconds that lapses before the device
	resends a request to the authentication server
Web-Based Param	Allow user login fail number. After login fail number exceed, the host will
(Max Login)	enter Lock state and is not able to authenticate until quiet period exceed.





Port	GE1-GE3	
Port Control	 Disabled Force Authorized Force Unauthorized Auto 	
Reauthentication	Enable	
Max Hosts	256	(1 - 256, default 256)
Common Timer		
Reauthentication	3600	Sec (300 - 2147483647, default 3600)
Inactive	60	Sec (60 - 65535, default 60)
Quiet	60	Sec (0 - 65535, default 60)
802.1x Parameters		
TX Period	30	Sec (1 - 65535, default 30)
Supplicant Timeout	30	Sec (1 - 65535, default 30)
Server Timeout	30	Sec (1 - 65535, default 30)
Max Request	2	(1 - 10, default 2)
Web-Based Parameter	'S	
Max Login	Infinite	(3 - 10, default 3)

- **Port :** Display selected Port number.
- > **Port Control :** Support following authentication port control types.
 - **Disable :** Disable authentication function and all clients have network accessibility.
 - Force Authorized : Port is force authorized and all clients have network accessibility.
 - Force Unauthorized : Port is force unauthorized and all clients have no network accessibility.
 - Auto : Need passing authentication procedure to get network accessibility.
- **Reauthentication :** Set checkbox to enable/disable reuauthentication.
- Max Hosts : In Multiple Authentication mode, total host number cannot not exceed max hosts number.
- **Common Timer:**

• **Reauthentication :** After re-authenticate period, host will return to initial state and need to pass authentication procedure again.



USER MANUAL



• Inactive : If no packet from the authenticated host, the inactive timer will increase. After inactive timeout, the host will be unauthorized and corresponding session will be deleted. In multi-host mode, the packet is counting on the authorized host only and not all packets on the port.

• Quiet : When port is in Locked state after authenticating fail several times, the host will be locked in quiet period. After this quiet period, the host is allowed to authenticate again.

• Auto : Need passing authentication procedure to get network accessibility.

802.1X Params :

• **TX Period :** Number of seconds that the device waits for a response to an Extensible Authentication Protocol (EAP) request/identity frame from the supplicant (client) before resending the request.

• **Supplicant Timeout :** The maximum number of EAP requests that can be sent. If a response is not received after the defined period (supplicant timeout), the authentication process is restarted.

• **Server Timeout:** Number of seconds that lapses before EAP requests are resent to the supplicant.

• **Max Request :** Number of seconds that lapses before the device resends a request to the authentication server.

• Max Login : Set checkbox to set max login number to be infinite or specify max login number.

Click the "Apply" button to save your changes or "Close" the button to close settings.





14.5.3 **MAC-Based Local Account**

Administrator can allow to add/edit/delete MAC-Based authentication local accounts, Setting

"add" and "Edit" and "Delete" function for this management.

Madamada						
Network	MAC-Based Local Account Table					
Port						
POE Setting	Show	ng All 🗸 entries		Showin	g 1 to 1 of 1 entries	
VLAN				VLAN	Timeout (Sec)	
MAC Address Table		MAC Address	Control		Reauthentication	Inactive
Spanning Tree		8C:4D:EA:FE:05:BE	Force Unauthorized	1	3600	60
Discovery		00.40.EA.T E.03.DE	Torce offaution2ed		5000	00
DHCP		Add Edit	Delete			
Multicast						
IP Configuration						
Security						
RADIUS						
TACACS+						
AAA						
Management Access						
Authentication Manager						
Property						
Port Setting MAC-Based Local Account						

Field	Description
	Authenticated host MAC address, and each MAC allow only one
MAC Address	entry in local database.
	Control Type
Control	 Force Authorized: Host will be force authorized.
	• Force Unauthorized: Host will be force unauthorized.
VLAN	Assigned VLAN ID for the authenticated host.
	Reauthentication: Assigned reauthentication period for
Timeout	the authenticated host.
	 Inactive: Assigned inactive timeout for the authenticated
	host.



dd MAC-Based Loca	I Account	
MAC Address	8C:4D:EA:FE:05:BE]
Port Control	 Force Authorized Force Unauthorized 	
VLAN	User Defined	(1 - 4094)
Assigned Timer		
Reauthentication	User Defined	Sec (300 - 2147483647)
Inactive	User Defined	Sec (60 - 65535)
Apply Close	•	

- \succ MAC Address : Authenticated host MAC address, and each MAC allow only one entry in local database.
- \geq **Port Control :** Support following authentication port control types.
 - Force Authorized: Host will be force authorized.
 - Force Authorized : Host will be force unauthorized.
- VLAN : Assigned VLAN ID for the authenticated host. \geq
- \geq **Assigned Timer:**
 - Timeout (Reauthentication) : Assigned reauthentication period for the authenticated host.
 - **Timeout (Inactive) :** Assigned inactive timeout for the authenticated host.





14.5.4 **WEB-Based Local Account**

Administrator can allow to add/edit/delete WEB-Based authentication local accounts, Setting "add" and "Edit" and "Delete" function for this management.

Status						
Network	WE	B-Based L	ocal A	count Table		
Port	-					
POE Setting	Snov	ving All 🗸 e	entries	Shov	ving 1 to 2 o	of 2 entries
VLAN				Timeout (Se	ec)	
MAC Address Table		Username	VLAN	Reauthentication	Inactive	
Spanning Tree		testusers	1	3600	60	
Discovery		testguest	1	3600	60	
DHCP		loonguoon				_
Multicast		Add	Edit	Delete		
P Configuration						
Security						
RADIUS						
TACACS+						
⊗ AAA						
Management Access						
 Authentication Manager Property 						
Port Setting						
MAC-Based Local Account						
in to based Local Account						

Field	Description	
Username	Authenticating account user name	
VLAN	Assigned VLAN ID for the authenticated host.	
	Reauthentication: Assigned reauthentication period for	
Timeout(Sec)	the authenticated host.Inactive: Assigned inactive timeout for the authenticated	
	host.	

Username	testguest	
Password	••••••	
Confirm Password	•••••	
	User Defined	
VLAN	1	(1 - 4094)
signed Timer		
Desuthersticetion	User Defined	
Reauthentication	3600	Sec (300 - 2147483647)
	User Defined	
Inactive	60	Sec (60 - 65535)

- \geq **Username** : Authenticating account user name.
- **Password :** Authenticating account password.
- \geq **Confirm Password :** Confirm authenticating account password.
- \geq **VLAN** : Assigned VLAN ID for the authenticated host.
- \geq **Assigned Timer:**
 - Timeout (Reauthentication) : Assigned reauthentication period for the

authenticated host.

Timeout (Inactive) : Assigned inactive timeout for the authenticated host.

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.5.5 Sessions

Administrator can check all detail information of authentication sessions and allow user to select specific session to delete by clicking "Clear" button.





Status						
Network	Sessions Ta	able				
Port		7				
POE Setting	Showing All	 entries 			Showing 0 to 0	of 0 ent
VLAN						
MAC Address Table	Session	ID Port	MAC Addre	ss Current	Type Status	
Spanning Tree						VLAN
Discovery						0 result
DHCP		_	_	_		
Multicast	Clear	Refresh				
IP Configuration						
Security						
RADIUS						
TACACS+						
AAA						
 Management Access Authentication Manager 						
Property						
Port Setting						
MAC-Based Local Account						
WEB-Based Local Account						
Sessions						
essions Table						
owing All 🗸 entries	Showing 0 to 0 of	0 entries			Q	
		Operatio	nal Information		Authorized Informa	tion
Session ID Port MAC Address	Current Type Status	/LAN Sessio Time		Quiet Time	Reauthentication Period	Inactive Timeou
	0 1	results found.				
				Fi	rst Previous 1	Next

Field	Description	
Session ID	Session ID is unique of each session	
Port	Port name which the host located	
MAC Address	Host MAC address	
Current Type	 Show current authenticating type 802.1x: Use IEEE 802.1X to do authenticating MAC-Based: Use MAC-Based authentication to do authenticating WEB-Based: Use WEB-Based authentication to do authenticating 	



	Show host authentication session status
	 Disable: This session is ready to be deleted
	 Running: Authentication process is running
	 Authorized: Authentication is passed and getting
-	network accessibility.
Status	 UnAuthorized: Authentication is not passed and not
	getting network accessibility.
	 Locked: Host is locked and do not allow to do
	authenticating until quiet period.
	• Guest: Host is in the guest VLAN.
	VLAN: Shows host operational VLAN ID.
	 Session Time: In "Authorized" state, it shows total time
	after authorized.
	 Inactived: In "Authorized" state, it shows how long the
Operationl	host do not send any packet.
	 Quiet Time: In "Locked" state, it shows total time after
	locked.
	 Locked: Host is locked and do not allow to do
	authenticating until quiet period.
	 VLAN: Shows VLAN ID given from authorized procedure
	 Reauthentication Period: Shows reauthentication
Authorized	period given from authorized procedure.
	 Inactive Timeouts: Shows inactive timeout given from
	authorized procedure.

Click the "Clear" button to clear this page or click the "Refresh" button to refresh the page.

14.6 Port Security

Port security examines all traffic received by secure ports to detect violations or to recognize and secure new MAC addresses. When the shutdown violation mode is configured, traffic cannot enter the secure port after a violation has been detected, which removes the possibility that violations might cause excessive CPU load.

Port security monitors received packets. Access to locked ports is limited to users with specific MAC addresses, This page allow user to configure port security settings for each interface. When port security is enabled on interface, action will be perform once MAC address over.

V1.0a



Security >> Port Security										
security is rort security										
Network	- Frank	644		Fachle						1
Port		Sta	ite 🔽	Enable	<u></u>					
POE Setting		Rate Lin	nit 10	0	Pa	cket / Se	ec (1 - 600, de	fault 100)		
VLAN										
MAC Address Table	A	pply	J							
Spanning Tree										
Discovery	Port	Secur	ity Tab	ole						
DHCP										
Multicast										
IP Configuration		Entry	Port	State	Address Limit	Total	Configured	Violate Number	Violate Action	Sticky
- Security		1	GE1	Enabled	20	0	Conngured 0		Protect	Enabled
RADIUS			GE1	Enabled	20	0		0	Protect	Disabled
TACACS+		2			1	-	0			
© AAA		3	GE3	Enabled	256	0	0	0	Restrict	Enabled
 Management Access Authorities Management 		4	GE4	Disabled	1	0	0	0	Protect	Disabled
 Authentication Manager Port Security 		5	GE5	Disabled	1	0	0	0	Protect	Disable
Protected Port		6	GE6	Disabled	1	0	0	0	Protect	Disable
Storm Control		7	GE7	Disabled	1	0	0	0	Protect	Disabled
© DoS		8	GE8	Disabled	1	0	0	0	Protect	Disabled
Oynamic ARP Inspection		9	GE9	Disabled	1	0	0	0	Protect	Disable
OHCP Snooping		10	GE10	Disabled	1	0	0	0	Protect	Disabled
IP Source Guard							-	-		

- State: Select the status of port security \triangleright
 - **Disable:** Disable port security function.
 - Enable: Enable port security function.
- \succ Rate Limit : Set rate limit of 1-600 packets per second.

	When the protect or restrict violation modes are configured, port security
	continues to process traffic after a violation occurs, which might cause
Note	excessive CPU load. Configure the port security rate limiter to protect the CPU
	against excessive load when the protect or restrict violation modes are
	configured.

Click the "Apply" button to save your changes settings.

Field	Description
Port	Port name which the port security.
State	Display port security of Enable or Disable state.
Addres Limie	Displays the maximum number of port security of MAC addresses that can be configured on the port.
Total	Displays the number of all port security total MAC addresses on the port.

V1.0a





Configured	Displays the number of all port security MAC addresses configured on the port.	
	Displays the operational state that the interface applies to	
	packets	
Violato Activo	arriving on the locked interface.	
/iolate Active	• Protect.	
	Restrict.	
	• Shutdown.	
Sticky	Display port security sticky of Enable or Disable.	

Port	GE1-GE5	
State	Enable	
Address Limit	1	(1 - 256, default 1)
Violate Action	 Protect Restrict Shutdown 	
Sticky	Enable	

- > **Port:** Display selected Port number.
- State: Enable or Un-Enable the port security.
- Address Limit: When configuring port security, the maximum number of secure MAC addresses that can be configured in the switch, A secure port has a default of one MAC address. The default can be changed to any value between 1 and 256. The upper limit of 256 guarantees one MAC address per port.
- Violate Action: Select the action if learned mac addresses, If Interface Status is locked, select an action to be applied to packets arriving on a locked interface.
 - **Protect:** Drop packets with invalid MAC address.
 - **Restrict:** Drop packets with invalid MAC address and log the event.
 - **Shutdown:** Drop packets with invalid MAC address and shut down the interface of port, and log the event.





14.7 Protected Port

This page allow user to configure protected port setting to prevent the selected ports from communication with each other. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port. If administrators check enable to make this a protected port. A protected port is also referred as a Private VLAN Edge. It's provide Layer 2 isolation between interfaces (Ethernet ports and Link Aggregation Groups) that share the same Broadcast domain (VLAN). After enable protected port, packets received from protected ports can be forwarded only to unprotected egress ports and unrestricted by VLAN members.

Security Protected Port	<u>u.</u>					
* Network	Prot	ected	Port Ta	able		
* Port						
POE Setting					Q	ſ
* VLAN		Entry	Port	State		
MAC Address Table		1	GE1	Protected		
 Spanning Tree 		2	GE2	Protected		
 Discovery 		3	GE3	Unprotected		
* DHCP				•		
 Multicast 		4	GE4	Unprotected		
* IP Configuration		5	GE5	Unprotected		
– Security		6	GE6	Unprotected		_
RADIUS		7	GE7	Unprotected		
TACACS+		8	GE8	Unprotected		
AAA		9	GE9	Unprotected		
 Management Access 		10	GE10	Unprotected		
Authentication Manager Rort Socurity		11	GE11	Unprotected		
Port Security Protected Port		12	GE12	Unprotected		





Edit I	Protected Port
	Port GE1-GE2
	State Protected
	pply Close

- > **Port:** Display selected Port number.
- State: Port protected admin state.
 - **Protected:** Enable protecting function.
 - Unprotected (deselect): Disable protecting function

14.8 Storm Control

When the rate of Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold, this function can to limit the number of frames entering the switch and to define the types of frames that are counted towards this limit. Will be the frames received beyond the threshold are discarded or the interface shuts down.

Security → Storm Contro status											
Network	1		O Pac	cket / Sec							
⊭ Port		Mode	🔘 Kbi	ts / Sec							
POE Setting			Exc	lude							
* VLAN		IFG		ude							
MAC Address Table											
Spanning Tree	A	pply									
Discovery											
* DHCP											
	Port	Softin	a Tabl								
 Multicast 	Port	Settin	g Tabl	le							
	Port	Settin	ig Tabl	le						0	
✓ Multicast	Port	Settin	ıg Tabl	le						۵	
MulticastIP Configuration	Port				Bro	adcast	Unknow	m Multicast	Unkno	Q wn Unicast	Action
Multicast Multicast IP Configuration Security	Port	Settin	ig Tabl	State	Bro	adcast Rate (Kbps)	Unknow State	m Multicast Rate (Kbps)	Unknov State		Action
Multicast IP Configuration Security RADIUS	Port									wn Unicast	Action
Multicast Multicast IP Configuration Security RADIUS TACACS+ AAA Management Access		Entry	Port	State	State	Rate (Kbps)	State	Rate (Kbps)	State	wn Unicast Rate (Kbps)	
Multicast Multicast IP Configuration Security RADIUS TACACS+ AAA Management Access Authentication Manager		Entry 1	Port GE1	State Disabled	State Disabled	Rate (Kbps) 10000	State Disabled	Rate (Kbps) 10000	State Disabled	wn Unicast Rate (Kbps) 10000	Drop Drop
Multicast Multicast IP Configuration Security RADIUS TACACS+ AAA Management Access		Entry 1 2	Port GE1 GE2	State Disabled Enabled	State Disabled Enabled	Rate (Kbps) 10000 10000	State Disabled Enabled	Rate (Kbps) 10000 10000	State Disabled Enabled	wn Unicast Rate (Kbps) 10000 10000	Drop

- Mode: Select the unit of storm control.
 - **Packets/sec:** Select by Packets/second of the rate threshold.
 - Kbits/sec: Select by Kbits/second of the rate threshold.





- IFG: Select the rate calculates w/o preamble & IFG (20 bytes). \succ
 - **Excluded:** exclude preamble & IFG (20 bytes) when count ingress storm control rate.
 - Include: include preamble & IFG (20 bytes) when count ingress storm control rate.

Click the "Apply" button to save your changes settings.

Field	Description
Port	Port name which the host located.
State	Display enable or disable the storm control function.
Broadcast	 Show the storm control for the Broadcast packets. State: Display enable or disable the storm control for broadcast packets. Rate(Kpps): Displays the bandwidth threshold for broadcast packets.
Unknown Multicast	 Show the storm control for the unknown Multicast packets. State: Display enable or disable the storm control for unknown Multicast packets . Rate(Kpps): Displays the bandwidth threshold for unknown Multicast packets.
Unknown Unicast	 Show the storm control for the unknown Unicast packets. State: Display enable or disable the storm control for unknown Unicast packets . Rate(Kpps): Displays the bandwidth threshold for unknown Unicast packets.
Action	 Drop: Shows will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold. Shutdown: will Broadcast / unknown Multicast or unknown Unicast frames is higher than the user-defined threshold.





Port	GE5,GE7	
State	🗹 Enable	
	🗹 Enable	
Broadcast	10000	Kbps (16 - 1000000, default 10000)
	🗌 Enable	
Unknown Multicast	10000	Kbps (16 - 1000000, default 10000)
	Enable	
Unknown Unicast	10000	Kbps (16 - 1000000, default 10000)
Action	Drop	

- **Port:** Display selected Port number. \geq
- State: Select the state of setting.
 - Enable: Enable the storm control function.
- \geq Broadcast: If enable storm control for Broadcast traffic will count Broadcast traffic towards the bandwidth threshold.
 - **Enable:** Enable the storm control function of Broadcast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- \geq Unknown Multicast: If enable storm control for unknown Multicast will count unknown Multicast traffic towards the bandwidth threshold.
 - Enable: Enable the storm control function of Unknown Multicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- \geq Unknown Unicast: If enable storm control for unknown Unicast will count unknown Unicast traffic towards the bandwidth threshold.
 - Enable: Enable the storm control function of Unknown Unicast packet, Value of storm control rate, Unit: Kbps (Kbits per-second, range16 - 1000000) depends on global mode setting.
- Action: Administrator can select Drop or Shutdown will Broadcast / unknown Multicast or \geq unknown Unicast frames is higher than the user-defined threshold.
 - **Drop:** Received beyond the threshold will discard the frames, Packets exceed storm control rate will be dropped
 - Shutdown: Received beyond the threshold will shut down the port, Port will be shutdown when packets exceed storm control rate.





14.9 DoS

DoS attack (denial-of-service) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

14.9.1 Property

This default is enabled all DoS protection feature and SYN-FIN / SYN-RST protections. The default threshold is 60 SYN packets per second. The default period of port recovery is 60 seconds.

DOD	Cashla
POD	Enable
Land	Enable
UDP Blat	C Enable
TCP Blat	Chable
DMAC = SMAC	C Enable
Null Scan Attack	
NUII SCAII ALIACK	Enable
X-Mas Scan Attack	Enable
TCP SYN-FIN Attack	Enable
	;
TCP SYN-RST Attack	C Enable
ICMP Fragment	C Enable
TCP-SYN	Enable
TOP-STR	Note: Source Port < 1024
	C Enable
TCP Fragment	
	Note: Offset = 1

	Enable IPv4	
Ping Max Size	Enable IPv6	
	512	Byte (0 - 65535, default 512)
TCP Min Hdr size	Enable	
TCP MIN HUT SIZE	20	Byte (0 - 31, default 20)
IDuć Min Francisco	Enable	
IPv6 Min Fragment	1240	Byte (0 - 65535, default 1240)
	Enable	
Smurf Attack	0	Netmask Length (0 - 32, default 0)
Apply		





- \triangleright POD:
 - **Enable:** Enable the Dos attack of avoids ping of death attack function.
- Land:
 - **Enable:** Enable the Dos attack of drops the packets if the source IP address is equal to the destination IP address function.
- \geq UDP Blat:
 - Enable: Enable the Dos attack of drops the packets if the UDP source port equals to the UDP destination port function.
- \geq TCP Blat:
 - **Enable:** Enable the Dos attack of drops the packages if the TCP source port is equal to the TCP destination port function.
- DMAC = SMAC: \geq
 - **Enable:** Enable the Dos attack of drops the packets if the destination MAC address is equal to the source MAC address function.
- Null Scan Attach: \geq
 - **Enable:** Enable the Dos attack of drops the packets with NULL scan function.
- \succ X-Mas Scan Attack:
 - **Enable:** Enable the Dos attack of drops the packets if the sequence number is zero, and the FIN, URG and PSH bits are set function.
- \geq **TCP SYN-FIN Attack:**
 - **Enable:** Enable the Dos attack of drops the packets with SYN and FIN bits set function.
- \geq TCP SYN-RST Attack:
 - **Enable:** Enable the Dos attack of drops the packets with SYN and RST bits set function.
- \succ ICMP Flagment:
 - **Drop:** Enable the Dos attack of drops the fragmented ICMP packets function.
- \geq TCP- SYN (SPORT<1024):
 - **Enable:** Enable the Dos attack of drops SYN packets with sport less than 1024 function.
- TCP Fragment (Offset = 1): \succ
 - **Enable:** Enable the Dos attack of drops the TCP fragment packets with offset equals to one function.
- \geq Ping Max Size:
 - **Enable:** Enable the Dos attack of specify the maximum size of the ICMPv4/ICMPv6 ping packets. The valid range is from 0 to 65535 bytes, and the default value is 512 bytes.
- **IPv4 Ping Max Size:** \geq
 - **Enable:** Enable the Dos attack of checks the maximum size of ICMP ping packets, and drops the packets larger than the maximum packet size function.





- \geq **IPv6 Ping Max Size:**
 - Enable: Enable the Dos attack of checks the maximum size of ICMPv6 ping packets, and drops the packets larger than the maximum packet size function.
- \geq TCP Min Hdr Size:
 - Enable: Enable the Dos attack of checks the minimum TCP header and drops the TCP packets with the header smaller than the minimum size. The length range is from 0 to 31 bytes, and default length is 20 bytes function.
- \geq **IPv6 Min Flagment:**
 - Enable: Enable the Dos attack of checks the minimum size of IPv6 fragments, and drops the packets smaller than the minimum size. The valid range is from 0 to 65535 bytes, and default value is 1240 bytes function.
- Smurf Attack: \geq
 - Enable: Enable the Dos attack of avoids smurf attack. The length range of the netmask is from 0 to 323 bytes, and default length is 0 bytes function.

Click the "Apply" button to save your changes settings

14.9.2 **Port Setting**

Administrator can choose protected ports.

Security ⇒ DoS ⇒ Port S status	cting				
Network	Port	Settin	ng Tabl	e	
⊭ Port			-		
POE Setting					Q,
¥ VLAN		Entry	Port	State	
MAC Address Table		1	GE1	Enabled	
Discovery		2	GE2	Enabled	
DHCP		3	GE3	Disabled	
Multicast		4	GE3	Disabled	
IP Configuration					
– Security		5	GE5	Disabled	
RADIUS		6	GE6	Disabled	
TACACS+		7	GE7	Disabled	
⊗ AAA		8	GE8	Disabled	
Management Access		9	GE9	Disabled	
 Authentication Manager Bost Occurity 		10	GE10	Disabled	
Port Security Protected Port		11	GE11	Disabled	
Storm Control		12	GE12	Disabled	
☆ DoS		13	GE13	Disabled	
Property		14	GE14	Disabled	
Port Setting		45	0545	Disabled	





Field	Description
Port	Interface of port number.
State	Display Enable/Disable the DoS protection on the interface.

Edi	t Port Se	tting	
_			
	Port	GE1-GE2	
	State	Enable	
_)(
	Apply	Close	

- **Port:** Display selected Port number. \succ
- \triangleright State: Select the state of setting.
 - Enable: Enable the DoS protection function.

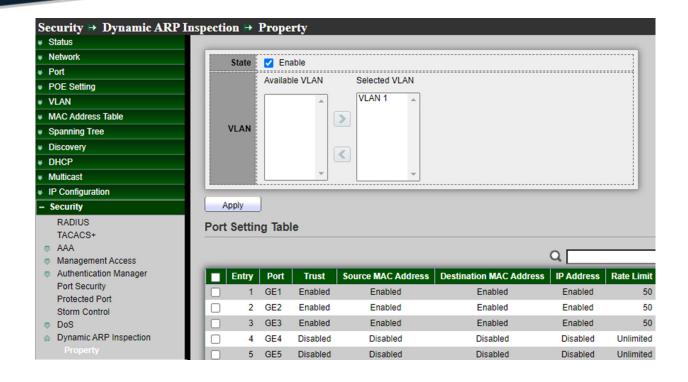
14.10 **Dynamic ARP Inspection**

Dynamic Address Resolution Protocol (ARP) is a TCP/IP protocol for translating IP addresses into MAC addresses. Use the Dynamic ARP Inspection pages to configure settings of Dynamic ARP Inspection.

14.10.1 **Property**

This page allow user to configure global and per interface settings of Dynamic ARP Inspection.





- State: Administrator can enable or disable this Dynamic ARP Inspection. Set checkbox to \geq enable/disable Dynamic ARP Inspection function.
- \geq VLAN: In the Enabled VLAN table, users assign static ARP Inspection lists to enabled VLANs. When a packet passes through an untrusted interface that is enabled for ARP Inspection switch will performs the checks, Select VLANs in left box then move to right to enable Dynamic ARP Inspection. Or select VLANs in right box then move to left to disable Dynamic ARP Inspection.

Click the "Apply" button to save your changes settings

Field	Description
Port	Port the port ID.
Trust	Display enable/disabled trust attribute of interface.
Source MAC Address	Display enable/disabled source mac address validation attribute of interface.
Destination MAC Address	Display enable/disabled destination mac address validation attribute of interface.





IP Address	Display enable/disabled IP address validation attribute of interface, Allow zero which means allow 0.0.0.0 IP address.
Rate Limit	Display rate limitation value of interface.

Port	GE1-GE3
Trust	Enable
Source MAC Address	Enable
Destination MAC Address	C Enable
IP Address	 Enable Allow Zero (0.0.0.0)
Rate Limit	50 pps (1 - 50, default 0), 0 is Unlimited

- Port: Display selected Port number.
- Trust: If enabled, the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests or replies sent to or from the interface. If Un-Enable, the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests or replies sent to or from the interface. By default, it is disabled.
- Source MAC Address: Check Enable to validate the source MAC addresses in ARP requests and replies, Set checkbox to enable or disable source mac address validation of interface. All ARP packets will be checked whether sender mac is same as source mac in Ethernet header if enable source mac address validation. Default is disabled.
- Destination MAC Address: Check Enable to validate the destination MAC addresses in ARP replies, Set checkbox to enable or disable destination mac address validation of interface. All ARP packets will be checked whether target mac is same as destination mac in Ethernet header if enable destination mac address validation. Default is disabled.
- IP Address: Set checkbox to enable or disable IP address validation of interface. All ARP packets will be checked whether IP address is 0.0.0.0,255.255.255.255 or multicast address. Default is disabled.
 - Allow all-zeros IP: If IP address validation is enabled, check Enable to allow 0.0.0.0 the IP address.
- Rate Limit: Enter the maximum rate that is allowed on the interface. The range is 1 to 50pps and the default is 0 Unlimited.





14.10.2 **Statistics**

The Statistics page will displays the statistical information for ARP Inspection.

Status									
Network	Stat	tistics	Table						
Port									
POE Setting								Q,	
VLAN		1	1		Source MAC	Destination MAC	Source IP	Destination IP	IP-MAC
MAC Address Table		Entry	Port	Forward	Failure	Failure	Validation Failure	Validation Failure	Mismatch Failu
Spanning Tree		1	GE1	0	0	0	0	0	
Discovery		2	GE2	0	0	0	0	0	
ЭНСР		3	GE3	0	0	0	0	0	
fulticast		4	GE4	0	0	0	0	0	
^o Configuration		-		-	-	•	-	-	
Security		5	GE5	0	0	0	0	0	
RADIUS		6	GE6	0	0	0	0	0	
TACACS+		7	GE7	0	0	0	0	0	
AAA		8	GE8	0	0	0	0	0	
Management Access		9	GE9	0	0	0	0	0	
Authentication Manager Port Security		10	GE10	0	0	0	0	0	
Protected Port		11	GE11	0	0	0	0	0	
Storm Control		12	GE12	0	0	0	0	0	
DoS		13	GE13	0	0	0	0	0	
Dynamic ARP Inspection		14	GE14	0	0	0	0	0	
Property		15	GE15	0	0	0	0	0	
Statistics					-	-	-		

Field	Description
Port	Interface of port number.
Forward	Display how many packets forwarded normally.
Source MAC Failure	Display how many packets dropped by source MAC validation.
Destination MAC Failure	Display how many packets dropped by destination MAC validation.
Source IP Address Validation Failures	Display how many packets dropped by source IP validation.
Destination IP Address Validation Failures	Display how many packets dropped by destination IP validation.
IP-MAC Mismatch Failures	Display how many packets dropped by IP-MAC doesn't match in IP Source Guard binding table.



DHCP Snooping 14.11

Administrator can use DHCP snooping to help avoid the Denial of Service attacks that result from unauthorized users adding a DHCP server to the network that then provides invalid configuration data to other DHCP clients on the network. DHCP packets received on other switch ports are inspected before being forwarded. Packets from untrusted sources are dropped.

14.11.1 Property

This page allow user to configure global and per interface settings of DHCP Snooping.

⊭ Status	ng → Property					
Network	State	🔽 Ena	ble			
⊭ Port		Availabl		Selected VL	A NI	
POE Setting				Selected VL	AN	
⊭ VLAN		VLAN 1	-		*	
MAC Address Table				>		
Spanning Tree	VLAN					
Discovery			0	<		
DHCP						
⊭ Multicast			~		*	
 IP Configuration 						
– Security	Apply					
RADIUS						
TACACS+	Port Settin	ng Table	e			
 AAA Management Access 		-				
 Management Access Authentication Manager 					Q	
Port Security	Entry	Port	Trust	Verify Chaddr	Rate Limit	
Protected Port	□ 1	GE1	Enabled	Enabled	45	
Storm Control © DoS	□ 2	GE2	Enabled	Enabled	45	
		GE3	Enabled	Enabled	45	
Dynamic ARP Inspection DHCP Snooping		GE4	Disabled	Disabled	Unlimited	

- State: Administrator can enable or Un-Enable DHCP Snooping, Set checkbox to enable/disable \geq DHCP Snooping function.
- \geq VLAN: Administrator can to enable DHCP Snooping on a VLAN, ensure that DHCP Snooping is globally enabled on the switch, Select VLANs in left box then move to right to enable DHCP Snooping. Or select VLANs in right box then move to left to disable DHCP Snooping.

Click the "Apply" button to save your changes settings.





Field	Description
Port	Interface of port number.
Trust	Display enable/disabled trust attribute of interface.
Verify Chaddr	Display enable/disabled chaddr validation attribute of interface.
Rate Limit	Display rate limitation value of interface.

Port	GE1-GE3		
Trust	Enable		
Verify Chaddr	Enable		
Rate Limit	45	pps (1 - 300, default 0), 0 is Unlimited	

- **Port:** Display selected Port number.
- Trust: If check Enable will connected to a DHCP server or to other switches or routers as trusted ports, Set checkbox to enable/disabled trust of interface. All DHCP packet will be forward directly if enable trust. Default is disabled
- Verify Chaddr: Set checkbox to enable or disable chaddr validation of interface. All DHCP packets will be checked whether client hardware mac address is same as source mac in Ethernet header if enable chaddr validation. Default is disabled.
- Rate Limit: Enter the maximum rate that is allowed on the interface. The range is 1 to 300pps and the default is 0 Unlimited.





Statistics 14.11.2

This page allow user to browse all statistics that recorded by DHCP snooping function.

Status								
Network	Stat	istics 1	Table					
Port								
POE Setting							Q	
VLAN							Untrust Port	
MAC Address Table		Entry	Port	Forward	Chaddr Check	Untrust Port	with Option82	Invalid
Spanning Tree					Drop	Drop	Drop	Drop
Discovery		1	GE1	0	0	0	0	0
DHCP		2	GE2	0	0	0	0	(
Multicast		3	GE3	0	0	0	0	(
P Configuration		4	GE4	0	0	0	0	(
Security		5	GE5	0	0	0	0	
RADIUS		6	GE6	0	0	0	0	(
TACACS+		-		-	-			
AAA		7	GE7	0	0	0	0	
Management Access Authentication Manager		8	GE8	0	0	0	0	
Port Security		9	GE9	0	0	0	0	(
Protected Port		10	GE10	0	0	0	0	(
Storm Control		11	GE11	0	0	0	0	(
DoS		12	GE12	0	0	0	0	(
Dynamic ARP Inspection		13	GE13	0	0	0	0	(
DHCP Snooping		14	GE14	0	0	0	0	(
Property Statistics		15	GE15	0	0	0	0	(

Field	Description
Port	Interface of port number.
Forward	Display how many packets forwarded normally.
Chaddr Check Drop	Display how many packets dropped by chaddr validation.
Untrusted Port Drop	Display how many DHCP server packets that are received by untrusted port dropped.
Untrusted Port with Option82 Drop	Display how many packets dropped by untrusted port with option82 checking.
Invalid Drop	Display how many packets dropped by invalid checking.





Option82 Property 14.11.3

This page allow user to set string of DHCP option82 remote ID filed. The string will attach in option82 if option inserted.

Security → DHCP Snoopi	ag → Op	tion82	Prop	erty		
* Status						
* Network	1			User Defin	ed	
✤ Port		Remote	ID			
* POE Setting						
* VLAN						
MAC Address Table	Op	eration	al Statu	IS		
 Spanning Tree 		Remote	ID 80	:4d:ea:30:do	d:53 (Switch Mac i	in Byte Order)
* Discovery			1			
* DHCP	A	pply				
 Multicast 						
 IP Configuration 	Port	Settin	g Tabl	e		
– Security						
RADIUS						Q
TACACS+		Entry	Port	State	Allow Untrust	
 AAA Management Access 		1	GE1	Disabled	Drop	
 Authentication Manager 		2	GE2	Disabled	Drop	
Port Security		3	GE3	Disabled	Drop	
Protected Port		4	GE4	Disabled	Drop	
Storm Control		5	GE5	Disabled	Drop	
 DoS Dynamic ARP Inspection 		6	GE6	Disabled	Drop	
 Dynamic ARP Inspection DHCP Snooping 		7	GE7	Disabled		
Property					Drop	
Statistics		8	GE8	Disabled	Drop	
Option82 Property		9	GE9	Disabled	Drop	

 \succ Remote ID: If Option 82 is enabled, select User Defined to manually enter the format remote ID, Set checkbox to enable user-defined remote-ID. By default, remote ID is switch mac in byte order.

Input user-defined remote ID. Only available when enable user-define remote ID.

Field	Description
Operational Status	Display remote ID information.

Click the "Apply" button to save your changes settings.





Field	Description
Port	Interface of port number.
State	Set checkbox to enable/disable option82 function of interface.
Allow untrusted	Display allow untrusted action of interface.

Edit Port Setting	
Port	GE1
State	Enable
Allow Untrust	 Keep Drop Replace
Apply C	Close

- \geq Port: Display selected Port number.
- \geq State: Check Enable or Un-Enable, Display option82 enable/disable status of interface.
- \geq Allow untrusted: Select the action perform when untrusted port receive DHCP packet has option82 filed. Default is drop.
 - Keep: Keep original option82 content.
 - Drop: Drop packets with option82.
 - **Replace:** Replace option82 content by switch setting.

14.11.4 **Option82 Circuit ID**

Administrator can use the Option82 Port CID Settings page to configure the Option 82 circuit-ID Setting "add" and "Edit" and "Delete" function management, This page allow user to set string of DHCP option82 circuit ID filed. The string will attach in option82 if option inserted.





Status	
Network	Option82 Circuit ID Table
⊧ Port	
POE Setting	Showing All entries Showing 0 to 0 of 0 entries Q
VLAN	Port VLAN Circuit ID
MAC Address Table	0 results found.
Spanning Tree	First Previous
Discovery	
DHCP	Add Edit Delete
Multicast	
IP Configuration	
- Security	
RADIUS TACACS+ AAA Management Access Authentication Manager Port Security Protected Port Storm Control DoS Dynamic ARP Inspection DHCP Snooping Property Statistics Option82 Property Option82 Circuit ID	

Field	Description	
Port	Display port ID of entry.	
VLAN	Display associate VLAN of entry.	
Circuit ID	Display circuit ID string of entry.	

Port	GE1 V	
VLAN	(1 - 4094) (Keep empty to set without VLAN)	
Circuit ID		

> **Port:** Select port from list to associate to CID entry. Only available on Add dialog.



- \geq VLAN: Input VLAN ID to associate to circuit ID entry. VLAN ID is not mandatory. Only available on Add dialog.
- \geq Dircuit ID: Input String as circuit ID. Packets match port and VLAN will be inserted circuit ID.

14.12 **IP Source Guard**

IP Source Guard restricts the client IP traffic to those source IP addresses configured in the IP Source binding database, mainly can prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

14.12.1 **Port Setting**

This page allow user to configure per port settings of IP Source Guard.

Security 🗩 IP Source Gua	rd 🔿 P	ort Set	tino				
status		ort oct	mg				
Network	Por	t Settin	g Tabl	e			
⊭ Port							
POE Setting							Q 🗌
VLAN		Entry	Port	State	Verify Source	Current Entry	Max Entr
MAC Address Table		1	GE1	Disabled	IP	Current Linuy 0	Unlimite
Spanning Tree		2	GE2	Enabled	IP-MAC	0	Unlimite
Discovery		2	GE2	Disabled	IP-WAC	0	Unlimite
DHCP			GE3 GE4		IP	0	
Multicast		4		Disabled			Unlimite
IP Configuration		5	GE5	Disabled	IP	0	Unlimite
- Security		6	GE6	Enabled	IP-MAC	0	Unlimite
RADIUS		7	GE7	Enabled	IP-MAC	0	Unlimite
TACACS+		8	GE8	Disabled	IP	0	Unlimite
© AAA		9	GE9	Disabled	IP	0	Unlimited
 Management Access Authentication Manager 		10	GE10	Disabled	IP	0	Unlimite
 Authentication Manager Port Security 		11	GE11	Disabled	IP	0	Unlimite
Protected Port		12	GE12	Disabled	IP	0	Unlimite
Storm Control		13	GE13	Disabled	IP	0	Unlimite
© DoS		14	GE14	Disabled	IP	0	Unlimite
Oynamic ARP Inspection		15	GE15	Disabled	IP	0	Unlimite
DHCP Snooping		16	GE16	Disabled	IP	0	Unlimite
 IP Source Guard Port Setting 		17	GE17	Disabled	IP	0	Unlimite
IMPV Binding					IP	0	
Save Database		18	GE18	Disabled	IP	0	Unlimite



Field	Description
Port	Interface of port number.
State	Display IP Source Guard enable/disable status of interface.
Verify Source	Display mode of IP Source Guard verification.
Current Binding Entry	Display current binding entries of a interface.
Max Binding Entry	Display the number of maximum binding entry of interface.

Port	GE2,GE6-GE7
State	🕑 Enable
Verify Source	 ○ IP ● IP-MAC
Max Entry	0 (1 - 50, default 0), 0 is Unlimited

- **Port:** Display selected Port number. \geq
- \geq State: Check Enable or Un-Enable this IP Source Guard. Mainly restricts the client IP traffic to those source IP addresses configured Check Enable to enable IP Source Guard on the interface. Administrator can disable this feature, Default is disabled.
- > Verify Source: Administrator can select IP only or MAC and IP type of source traffic to be verified.
 - **IP:** Only verify source IP address of packet.
 - IP-MAC: Verify source IP and source MAC address of packet
- Max Entry: Administrator need enter the maximum number of IP source binding rules. The \geq range is 0 to 50, and 0 is Unlimited.





IMPV Binding 14.12.2

Use the Binding to query and view information about inactive addresses recorded in the IP Source Guard database, This page allow user to add static IP source guard entry and browse all IP source guard entries that learned by DHCP snooping or statically create by user, Setting "add" and "Edit" and "Delete" for this function management.

Security >> IP Source Guar	rd 🗭 IMPV Bindi	ng			
Network	IP-MAC-Port-V	LAN Binding Table	e		
✤ Port					
POE Setting	Showing All 🗸 e	ntries	Showing 1 to 1 of 1 entries	Q	
* VLAN	Port VLA	MAC Address	IP Address	Binding	Type Lease Time
MAC Address Table	GE1 409		192.168.2.55 / 255.255.255.255	IP-MAC-Port-VLAN	Static N/A
 Spanning Tree 	10 GET 409	4 00.4D.EA.FE.05.A9	192.108.2.007.200.200.200		
* Discovery	Add]	Edit Delete		First	revious 1 Next L
* DHCP					
 Multicast 					
IP Configuration					
– Security					
RADIUS					
TACACS+					
AAA					
Management Access					
Authentication Manager					
Port Security Protected Port					
Storm Control					
© DoS					
 Dynamic ARP Inspection 					
DHCP Snooping					
IP Source Guard					
Port Setting					
IMPV Binding					

Field	Description		
Port	Display port ID of entry.		
VLAN	Display VLAN ID of entry.		
MAC Address	Display MAC address of entry. Only available of IP-MAC binding entry.		
IP Address	Display IP address of entry. Mask always to be 255.255.255.255 IP-MAC binding. IP binding entry display user input		
Binding	Display binding type of entry.		
Status	 Type of existing binding entry: Static : Entry added by user manually configured. Dynamic : Entry learned by DHCP snooping. 		





_	
Lease	Time

Lease time of DHCP Snooping learned entry. After lease time entry will be deleted. Only available of dynamic entry.

Port	GE1 🗸		
VLAN	4094	(1 - 4094)	
Binding	IP-MAC-Port-VLAN IP-Port-VLAN		
MAC Address	8C:4D:EA:FE:05:A9		
IP Address	192.168.2.55	/ 255.255.255.255	

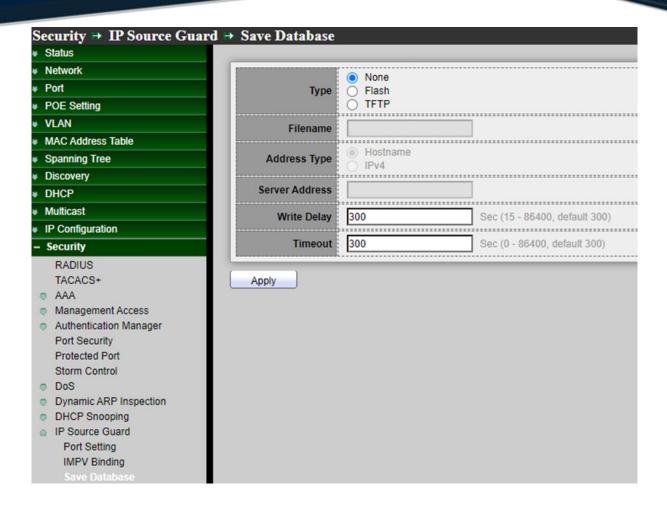
- \geq **Port:** Administrator can select port from list of a binding entry.
- \geq VLAN: Specify a VLAN ID of a binding entry.
- \geq Binding: Administrator can select matching mode of binding entry.
 - **IP-MAC-Port-VLAN:** packet must match IP address MAC address Port and VLAN ID.
 - **IP-Port-VLAN:** packet must match IP address or subnet \rightarrow Port and VLAN ID.
- MAC Address: Input MAC address. Only available on IP-MAC-Port-VLAN mode. \geq
- \geq **IP Address:** Input IP address and mask. Mask only available on IP-MAC-Port mode.

Click the "Apply" button to save your changes or "Close" the button to close settings.

14.12.3 Save Databases

This page allow user to configure DHCP snooping database which can backup and restore dynamic DHCP snooping entries





- \geq **Type:** Administrator can select the type of database agent.
 - None: Disable database agent service.
 - Flash: Save DHCP dynamic binding entries to flash.
 - **TFTP:** Save DHCP dynamic binding entries to remote TFTP server.
- \geq Filename: Set file name of TFTP server, Input filename for backup file. Only available when selecting type "flash" and "TFTP".
- \geq Address Type: Select use Host name or IP address to connection TFTP server.
 - Hostname: TFTP server address is hostname.
 - IPv4: TFTP server address is IPv4 address.
- Server Address: Input remote TFTP server hostname or IP address. Only available when \geq selecting type "TFTP.
- \geq Write Delay: Input delay timer for doing backup after change happened. Default is 300 seconds.
- Timeout: Input aborts timeout for doing backup failure. Default is 300 seconds. \geq

Click the "Apply" button to save your changes settings.





15. ACL

Note

ACL (Access Control List) is an ordered list of classification filters and actions. Each single classification rule, together with its action, is called an Access Control Element (ACE). Each ACE is made up of filters that distinguish traffic groups and associated actions. A single ACL may contain one or more ACEs, which are matched against the contents of incoming frames. Either a DENY or PERMIT action is applied to frames whose contents match the filter.

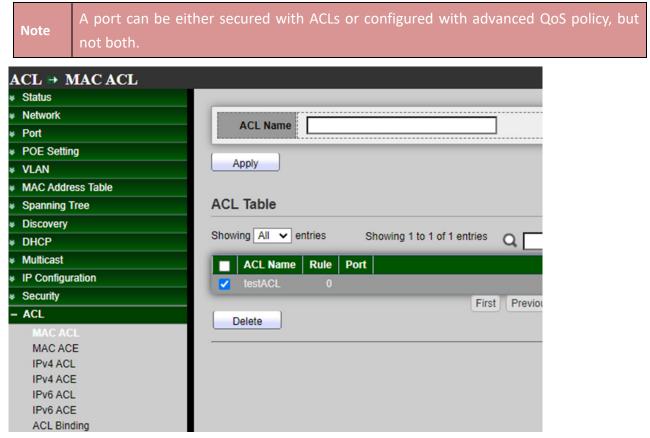
When a packet matches an ACE filter, the ACE action is taken and that ACL processing is stopped. If the packet does not match the ACE filter, the next ACE is processed. If all ACEs of an ACL have been processed without finding a match, and if another ACL exists, it is processed in a similar manner.

If no match is found to any ACE in all relevant ACLs then ACL default action will dropped the packet.

15.1 MAC ACL

This page mainly creates MAC ACLs profile. The MAC ACLs are used to filter traffic based on Layer 2 fields and defined on the MAC ACE page.

This page allow user to add or delete ACL rule. A rule cannot be deleted if under binding.



V1.0a





 \triangleright ACL Name: Create a name of ACL.

Click the "Apply" button to save your changes settings.

Field	Description
ACL Name	Display MAC ACL name.
Rule	Display the number ACE rule of ACL
Port	L Display the port list that bind this ACL.

Click the "Delete" button to delete ACL table list.

15.2 MAC ACE

MAC ACE will check all frames for a match. Setting "add" and "Edit" and "Delete" for this function management, This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding .

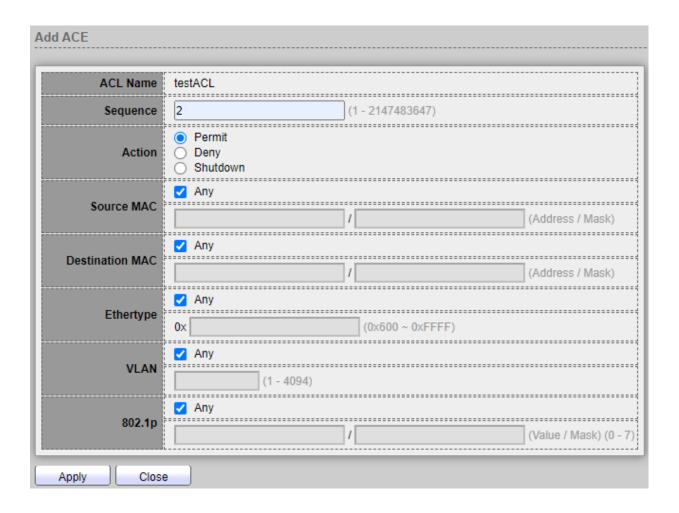
Status											
Network	ACE	Table									
Port											
POE Setting	ACL	Name testA	CL 🗸								
VLAN	Show	/ing All 🗸	entries		Shov	ving 1 to 1 o	f 1 entries				
MAC Address Table					0.101	ing rio ro				Q	
Spanning Tree	_	Sequence	Action	Source	MAC	Destinatio	on MAC	Ethertype	VLAN	802	.1 p
Discovery		Sequence	Action	Address	Mask	Address	Mask	Eulenype	VLAN	Value	Mas
DHCP		2	Permit	Any	Any	Any	Any	Any	Any	Any	An
Multicast		A.4.)[E .(1)	10 0	1				First	Previo	ous
IP Configuration		Add	Edit		elete						
Security											
ACL											
MAC ACL											
MAC ACE											

 \geq ACL Name: Select the ACL name to which an ACE is being added.





Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE
Source MAC	Display the source MAC address and mask of ACE.
Destination MAC	Display the destination MAC address and mask of ACE.
Ethertype	Display the Ethernet frame type of ACE.
VLAN ID	Display the VLAN ID of ACE
802.1p Value	Display the 802.1p value of ACE.
802.1p Mask	Display the 802.1p mask of ACE.



 \triangleright ACL Name: Display the ACL name to which an ACE is being added.





- \geq **Sequence:** ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- \geq Action: Administrator can select the action after ACE match packet.
 - Permit: Forward packets that meet the ACE criteria.
 - **Deny:** Drop packets that meet the ACE criteria.
 - **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- \geq Source MAC: Select the type for source MAC address.
 - **Any:** All source addresses are acceptable.
 - User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source MAC address and mask to which will be matched.
- **Destination MAC:** Destination MAC Select the type for Destination MAC address. \geq
 - Any: All destination addresses are acceptable.
 - **User Defined:** Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination MAC address and mask to which will be matched.

Note MAC address are used(8C:4D:EA).

- \geq **Ethertype:** Select the type for Ethernet frame type.
 - **Any:** All Ethernet frame type is acceptable.
 - **User Defined:** Only an Ethernet frame type which users define is acceptable. Enter the Ethernet frame type value to which will be matched.
- \geq VLAN ID: Select the type for VLAN ID.
 - Any: All VLAN ID is acceptable.
 - User Defined: User Defined: Only a VLAN ID which users define is acceptable. Enter the VLAN ID to which will be matched.
- **802.1p:** Select the type for 802.1p value. \geq
 - Any: All 802.1p value is acceptable.
 - User Defined: User Defined: Only an 802.1p value or a range of 802.1p value which users define is acceptable. Enter the 802.1p value and mask to which will be matched.





15.3 IPv4 ACL

Mainly creates IPv4 ACLs profile. The IPv4 ACLs are used to check IPv4 packets, This page allow user to add or delete Ipv4 ACL rule. A rule cannot be deleted if under binding.

ACL → IPv4 ACL		
* Network	A CL Name	
✤ Port	ACL Name	
POE Setting		
* VLAN	Apply	
MAC Address Table		
 Spanning Tree 	ACL Table	
* Discovery		
* DHCP	Showing All v entries Showing 1 to 1 of 1 entries	Q
 Multicast 	ACL Name Rule Port	
IP Configuration	v test 0	
 Security 	(First Previous
– ACL	Delete	
MAC ACL		
MAC ACE		
IPv4 ACL		

ACL Name: Create a name of ACL. >

Click the "Apply"	button to save yo	our changes settings.
-------------------	-------------------	-----------------------

Field	Description
ACL Name	Display IPv4 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

Click the "Delete" button to delete the table list.

15.4 IPv4 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting "add" and "Edit" and "Delete" for this function management.





ACL → IPv4 ACE		
✤ Network	ACE Table	
✤ Port	ACI Nama Itati	
 POE Setting 	ACL Name test V	
* VLAN	Showing All v entries	Showin
MAC Address Table		
 Spanning Tree 	Source IP Sequence Action Protocol	Desti
* Discovery	Address Mask	Addres
* DHCP		
 Multicast 	Add Edit Delete	
* IP Configuration		
* Security		
– ACL		
MAC ACL		
MAC ACE		
IPv4 ACL		
IPv4 ACE		

 \succ **ACL Name:** Select the ACL name to which an ACE is being added.

ACE	E Table													
ACLI	ACL Name test V													
Show	Showing All v entries Showing 0 to 0 of 0 entries													
	Sequence	Action	Protocol	Source	IP	Destinat	tion IP	Source Port	Destination Port	TCP Flags	Тур	e of Service	ICN	
	Sequence	Action	Protocol	Source Address				Source Port	Destination Port	TCP Flags				
	Sequence	Action	Protocol				Mask	Source Port 0 results found.	Destination Port	TCP Flags				

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.
Source IP	Display the source IP address and mask of ACE:Address: Display for the IPv4 IP address.
	 Mask : Display for the Mask address.
Destination IP	Display the destination IP address and mask of ACE:



Add ACF



 Address: Display for the IPv4 IP address.
 Mask : Display for the Mask address.
Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
Display the TCP flag value if ACE. Only available when protocol is TCP.
Display the ToS value of ACE which could be DSCP or IP Precedence.
Display the ICMP type and code of ACE. Only available when protocol is ICMP.

ACL Name	test	
Sequence	(1 - 2147483647)	
Action	 Permit Deny Shutdown 	
Protocol	Any Select ICMP	
	O Define (0 - 255)	
Source IP	🗹 Any	
Source IP		(Address / Mask)
	Any Any	
Destination IP	/	(Address / Mask)
	Any	
Type of Service	O DSCP (0 - 63)	
	O IP Precedence (0 - 7)	

- > ACL Name: Display the ACL name to which an ACE is being added.
- Sequence: Specify the sequence of the ACE ,ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- > Action: Administrator can select the action for a match.





- **Permit:** Forward packets that meet the ACE criteria.
- **Deny:** Drop packets that meet the ACE criteria.
- **Shutdown:** Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- **Protocol:** Administrator can select the type of protocol for a match. \geq
 - Any (IP): All IP protocols are acceptable.
 - **Select from list:** Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/ RSVP/IPV6:ICMP/OSPF/PIM/L2TP)
 - Protocol ID to match: Enter the protocol ID.
- \geq **Source IP:** Select the type for source IP address.
 - Any: All source addresses are acceptable.
 - **User Defined:** Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.
- Destination IP: Select the type for destination IP address.. \geq
 - Any: All destination addresses are acceptable.
 - User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and mask to which will be matched.
- **Type of Service:** Select the type of service for a match. \geq
 - **Any:** All types of service are acceptable.
 - **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match. •
 - IP Precedence to match: Enter a IP Precedence to match.





	Any
Source Port	Single (0 - 65535)
	Range (0 - 65535)
	Any
Destination Port	O Single (0 - 65535)
	Range (0 - 65535)
	Urg: 🔿 Set 🔿 Unset 🖲 Don't care
	Ack: 🔿 Set 🔿 Unset 🖲 Don't care
TCP Flags	Psh: 🔿 Set 🔿 Unset 🖲 Don't care
	Rst: 🔿 Set 🔿 Unset 🖲 Don't care
	Syn: 🔿 Set 🔵 Unset 🖲 Don't care
	Fin: 🔿 Set 🔿 Unset 💿 Don't care
	Any
ICMP Type	O Select Echo Reply
	O Define (0 - 255)
ICMP Code	Any
ICMP Code	O Define (0 - 255)
Apply Clos	e

- Source Port: Select the type of protocol for a match. Only available when protocol is TCP or UDP.
 - Any: All source ports are acceptable.
 - **Single:** Enter a single TCP/UDP source port to which packets are matched.
 - **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- Destination Port: Select the type of protocol for a match. Only available when protocol is TCP or UDP.
 - Any: All source ports are acceptable.
 - **Single:** Enter a single TCP/UDP source port to which packets are matched.
 - **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- TCP Flags: Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.





- Set: Match if the flag is SET.
- Unset: Match if the flag is Not SET.
- Don't care: Ignore the TCP flag.
- \geq ICMP Type: Either select the message type by name or enter the message type number. Only available when protocol is ICMP.
 - **Any:** All message types are acceptable.
 - Select from list: Select message type by name.
 - Protocol ID to match: Enter the number of message type.
- \geq ICMP Code: Select the type for ICMP code. Only available when protocol is ICMP.
 - Any: All codes are acceptable.
 - User Defined: Enter an ICMP code to match.

Click the "Apply" button to save your changes or "Close" the button to close settings.

15.5 IPv6 ACL

Mainly creates IPv6 ACLs profile. The IPv6 ACLs are used to check IPv6 packets, This page allow user to add or delete Ipv6 ACL rule. A rule cannot be deleted if under binding.

ACL → IPv6 ACL		ľ
* Status		
* Network	ACL Name	
✤ Port		
 POE Setting 		
* VLAN	Apply	
 MAC Address Table 		
 Spanning Tree 	ACL Table	
* Discovery		
* DHCP	Showing All entries Showing 0 to 0 of 0 entries	
* Multicast	ACL Name Rule Port	
* IP Configuration	0 results found.	
* Security		First
– ACL	Delete	(not
MAC ACL		
MAC ACE		
IPv4 ACL		
IPv4 ACE		
IPv6 ACL		

ACL Name: Create a name of ACL. \geq

Click the "Apply" button to save your changes settings.

V1.0a



Field	Description
ACL Name	Display IPv6 ACL name
Rule	Display the number ACE rule of ACL
Port	Display the port list that bind this ACL

Click the "Delete" button to delete the table list.

15.6 IPv6 ACE

This page allow user to add, edit or delete ACE rule. An ACE rule cannot be edited or deleted if ACL under binding. New ACE cannot be added if ACL under binding, Setting "add" and "Edit" and "Delete" for this function management.

ACL 🖶 IPv6 ACE								
⊌ Status								
Network	ACE	Table						
✤ Port								
POE Setting	ACL	Name None	~					
* VLAN	Show	ring All 🗸 e	entries				Showing	0 to 0 of
MAC Address Table								
 Spanning Tree 		Sequence	Action	Protocol	Sourc	e IP	Destina	tion IP
 Discovery 		Sequence	ACUON	PIOLOCOI	Address	Prefix	Address	Prefix
* DHCP								
 Multicast 	_							-
IP Configuration								
* Security								
– ACL								
MAC ACL								
MAC ACE								
IPv4 ACL								
IPv4 ACE								
IPv6 ACL								
IPv6 ACE								

 \succ ACL Name: Select the ACL name to which an ACE is being added.



ACE	Table																
	lame None	~															
how	ing All 🗸 e	entries				Show	ring 0 to 0) of 0 entries					Q				
_	Sequence	Antina	Destand	Sourc	e IP	Destination IP		Source Port Destinction Port				Source Port Destination Port TCP Flag		Тур	e of Service	IC	мр
	sequence	Action	Protocol	Address	Prefix	Address	Prefix	Source Port	Desunation Port	ICP riags	DSCP	IP Precedence	Туре	Code			
	0 results found.																

Field	Description
Sequence	Display the sequence of ACE.
Action	Display the action of ACE.
Protocol	Display the protocol value of ACE.
Source IP	 Display the source IP address and mask of ACE: Address: Display for the IPv4 IP address. Mask : Display for the Mask address.
Destination IP	 Display the destination IP address and mask of ACE: Address: Display for the IPv4 IP address. Mask : Display for the Mask address.
Source Port	Display single source port or a range of source ports of ACE. Only available when protocol is TCP or UDP.
Destination Port	Display single destination port or a range of destination ports of ACE. Only available when protocol is TCP or UDP.
TCP Flags	Display the TCP flag value if ACE. Only available when protocol is TCP.
Type of Service	Display the ToS value of ACE which could be DSCP or IP Precedence.
ICMP	Display the ICMP type and code of ACE. Only available when protocol is ICMP.





Add ACE	
ACL Name	test1122
Sequence	(1 - 2147483647)
Action	 Permit Deny Shutdown
Protocol	 Any Select TCP Define (0 - 255)
Source IP	Any (Address / Prefix (0 - 128))
Destination IP	Any Any (Address / Prefix (0 - 128))
Type of Service	Any DSCP (0 - 63) IP Precedence (0 - 7)

- ACL Name: Display the ACL name to which an ACE is being added. \geq
- \geq Sequence: Specify the sequence of the ACE, ACEs with higher sequence are processed first (1 is the highest priority). Only available on Add Dialog.
- \geq **Action:** Administrator can select the action for a match.
 - **Permit:** Forward packets that meet the ACE criteria.
 - **Deny:** Drop packets that meet the ACE criteria.
 - Shutdown: Drop packets that meet the ACE criteria, and disable the port from where the packets were received. Such ports can be reactivated from the Port Settings page.
- \geq **Protocol:** Administrator can select the type of protocol for a match.
 - Any (IP): All IP protocols are acceptable.
 - **Select from list:** Select one of the following protocols from the drop-down list. (ICMP/IPinIP/TCP/EGP/IGP/UDP/HMP/RDP/IPV6/IPV6:ROUT/IPV6:FRAG/ RSVP/IPV6:ICMP/OSPF/PIM/L2TP)
 - **Protocol ID to match:** Enter the protocol ID.
- **Source IP:** Select the type for source IP address. \geq
 - Any: All source addresses are acceptable.
 - User Defined: Only a source address or a range of source addresses which users define are acceptable. Enter the source IP address value and mask to which will be matched.

+(886) 2-8911-6160





- \geq Destination IP: Select the type for destination IP address..
 - Any: All destination addresses are acceptable.
 - User Defined: Only a destination address or a range of destination addresses which users define are acceptable. Enter the destination IP address value and prefix to which will be matched.
- \geq **Type of Service:** Select the type of service for a match.
 - **Any:** All types of service are acceptable.
 - **DSCP to match:** Enter a Differentiated Serves Code Point (DSCP) to match. •
 - IP Precedence to match: Enter a IP Precedence to match.

	Any	
Source Port	O Single	(0 - 65535)
	🔿 Range	- (0 - 65535)
	Any	
Destination Port	O Single	(0 - 65535)
	🔿 Range	- (0 - 65535)
	Urg: 🔵 Set 🔵 Unset 🔘 Don't care	
	Ack: 🔿 Set 🔿 Unset 💿 Don't care	
TCD Flags	Psh: 🔵 Set 🔵 Unset 🔘 Don't care	
TCP Flags	Rst: 🔿 Set 🔿 Unset 💿 Don't care	
	Syn: 🔵 Set 🔵 Unset 🖲 Don't care	
	Fin: 🔵 Set 🔵 Unset 🍥 Don't care	
	Any	
ICMP Type	○ Select Destination Unreachable ✓	
	O Define	(0 - 255)
ICMP Code	Any	
	O Define	(0 - 255)
Apply Clos	e	

 \geq **Source Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.

- **Any:** All source ports are acceptable.
- **Single:** Enter a single TCP/UDP source port to which packets are matched.
- **Range:** Select a range of TCP/UDP source ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- \succ **Destination Port:** Select the type of protocol for a match. Only available when protocol is TCP or UDP.

V1.0a





- Any: All source ports are acceptable.
- **Single:** Enter a single TCP/UDP source port to which packets are matched.
- **Range:** Select a range of TCP/UDP destination ports to which the packet is matched. There are eight different port ranges that can be configured (shared between source and destination ports). TCP and UDP protocols each have eight port ranges.
- TCP Flags: Select one or more TCP flags with which to filter packets. Filtered packets are either forwarded or dropped. Filtering packets by TCP flags increases packet control, which increases network security. Only available when protocol is TCP.
 - Set: Match if the flag is SET.
 - Unset: Match if the flag is Not SET.
 - **Don't care:** Ignore the TCP flag.
- ICMP Type: Either select the message type by name or enter the message type number. Only available when protocol is ICMP.
 - Any: All message types are acceptable.
 - Select from list: Select message type by name.
 - **Protocol ID to match:** Enter the number of message type.
- > ICMP Code: Select the type for ICMP code. Only available when protocol is ICMP.
 - Any: All codes are acceptable.
 - User Defined: Enter an ICMP code to match.

Click the "Apply" button to save your changes or "Close" the button to close settings.

15.7 ACL Binding

This page allow user to bind or unbind ACL rule to or from interface. IPv4 and Ipv6 ACL cannot be bound to the same port simultaneously, Administrator can from ACL Binding Table to select ports. When an ACL is bound to an interface, its ACE rules are applied to packets arriving at that interface. Packets that do not match any of the ACEs in the ACL are matched to a default rule, whose action is to drop unmatched packets.



ACT > ACT P-



ACL ACL Binding						
 Status 						
Network	ACL	Bindi	ng Tab	le		
✤ Port	_					
POE Setting						
¥ VLAN		Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
MAC Address Table		1	GE1	testACL		
 Spanning Tree 		2	GE2	testACL		
 Discovery 		3	GE3	testACL		
* DHCP				IESIACE		
 Multicast 		4	GE4			
 IP Configuration 		5	GE5			
		6	GE6			
– ACL		7	GE7			
MAC ACL		8	GE8			
MAC ACE		9	GE9			
IPv4 ACL		10	GE10			
IPv4 ACE		11	GE11			
IPv6 ACL		12	GE12			
IPv6 ACE		13	GE13			
ACL Binding		10	0210			

Field	Description
Port	Display port entry ID.
MAC ACL	Display mac ACL name that bound of interface. Empty means no rule bound.
IPv4 ACL	Display ipv4 ACL name that bound of interface. Empty means no rule bound.
IPv6 ACL	Display ipv6 ACL name that bound of interface. Empty means no rule bound.



Dent	GE1-GE3
Port	Note: ACL without any rules cannot be bound
MAC ACL	testACL 🗸
IPv4 ACL	None 🗸
IPv6 ACL	None 🗸

- \geq Port: Displays selected Port number.
- MAC ACL: MAC ACLs that are bound to the interface, Select mac ACL name from list to bind. \geq
- \geq IPv4 ACL: IPv4 ACLs that are bound to the interface, Select IPv4 ACL name from list to bind.
- IPv6 ACL: IPv6 ACLs that are bound to the interface, Select IPv6 ACL name from list to bind. \geq

Click the "Apply" button to save your changes or "Close" the button to close settings.

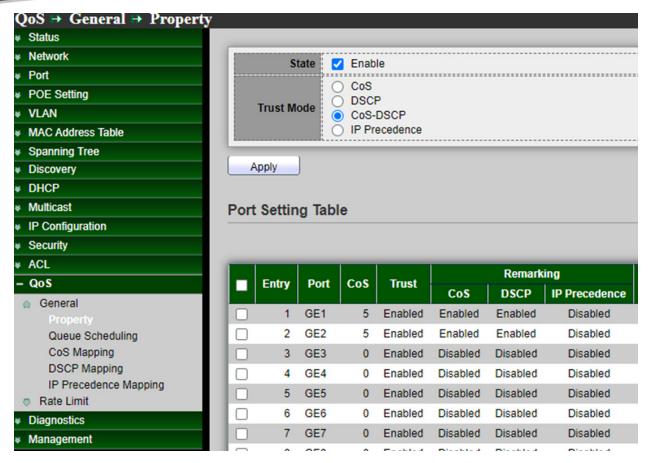
16. QoS

The quality of service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and the desired traffic receives preferential treatment.

16.1 Property

The QoS feature is used to optimize network performance, Use the QoS general pages to configure settings for general purpose





- State: Administrator can enable or disable this QoS Feature.
 - **Trust Mode:** Administrator can select CoS / DSCP / CoS-DSCP and IP Precedence mode.
 - **CoS:** Traffic is mapped to queues based on the CoS field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the CoS to queue can be configured on port setting dialog.
 - **DSCP:** All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue can be configured on the DSCP mapping page. If traffic is not IP traffic, it is mapped to the best effort queue..
 - **CoS-DSCP:** Select to use Trust CoS mode for non-IP traffic and Trust DSCP mode for IP traffic.
 - IP Precedence: Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence mapping page.

Click the "Apply" button to save your changes settings.





Field	Description						
Port	Interface of port name.						
CoS	Port default CoS priority value for the selected ports.						
	Port trust state:						
Trust	 Enabled: Traffic will follow trust mode in global setting. 						
	• Disabled: Traffic will always use best efforts.						
	Remarking (CoS) Port CoS remaking admin state:						
Remarking (CoS)	Enabled: CoS remarking is enabled.						
	• Disabled: CoS remarking is disabled.						
	Port DSCP remaking admin state:						
Remarking (DSCP)	Enabled: DSCP remarking is enabled.						
	• Disabled: DSCP remarking is disabled.						

Edit Port Setting	
Port	GE1-GE2
CoS	5 (0 - 7)
Trust	Enable
Remarking	
CoS	Enable
DSCP	🗹 Enable
IP Precedence	Enable
Apply CI	lose

- Port: Displays selected port number. \geq
- \succ **CoS:** Set default CoS/802.1p priority value for the selected ports, Set the default CoS value to be assigned for incoming packets (that do not have a VLAN tag). The range is 0 to 7.
- \geq **Trust:** Set checkbox to enable/disable port trust state.
- \geq **Remarking:**
 - CoS: Set checkbox to enable/disable port CoS remarking, Traffic is mapped to queues based on the VPT field in the VLAN tag, or based on the per-port default CoS value (if there is no VLAN tag on the incoming packet), the actual mapping of the VPT to queue can be configured on the CoS to Queue page.
 - DSCP: Set checkbox to enable/disable port DSCP remarking,All IP traffic is mapped to queues based on the DSCP field in the IP header. The actual mapping of the DSCP to queue

V1.0a





can be configured on the DSCP to Queue page. If traffic is not IP traffic, it is mapped to the best effort queue.

• IP Precedence: Set checkbox to enable/disable port IP Precedence remarking, Traffic is mapped to queues based on the IP precedence. The actual mapping of the IP precedence to queue can be configured on the IP Precedence to Queue page.

Click the "Apply" button to save your changes or "Close" the button to close settings.

16.2 Queue Scheduling

The switch supports eight queues for each interface. Queue number 8 is the highest priority queue. Queue number 1 is the lowest priority queue. There are two ways of determining how traffic in queues is handled, Strict Priority (SP) and Weighted Round Robin (WRR).

• Strict Priority (SP)—Egress traffic from the highest priority queue is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, which provide the highest level of priority of traffic to the highest numbered queue.

• Weighted Round Robin (WRR)—In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight, the more frames are sent).

The queuing modes can be selected on the Queue page.When the queuing mode is by Strict Priority, the priority sets the order in which queues are serviced, starting with queue_8 (the highest priority queue) and going to the next lower queue when each queue is completed.

When the queuing mode is Weighted Round Robin, queues are serviced until their quota has been used up and then another queue is serviced. It is also possible to assign some of the lower queues to WRR, while keeping some of the higher queues in Strict Priority. In this case traffic for the SP queues is always sent before traffic from the WRR queues. After the SP queues have been emptied, traffic from the WRR queues is forwarded. (The relative portion from each WRR queue depends on its weight).





 Network Port POE Setting VLAN MAC Address Table Spanning Tree Discovery DHCP Multicast Security ACL Queue Scheduling Table Method Strict Priority WRR Weight WRR Bandwidth (% 1 0 1 33.33% 2 0 1 33.33% 2 0 2 66.67% 3 0 3 4 0 4 0 4 0 4 0 4 0 3 15 	Status					
POE Setting VLAN MAC Address Table Spanning Tree Discovery DHCP Multicast IP Configuration Security ACL Queue ACL ACL <th>Network</th> <th>Queue</th> <th>Scheduling</th> <th>Table</th> <th></th> <th></th>	Network	Queue	Scheduling	Table		
VLAN MAC Address Table Spanning Tree Discovery DHCP Multicast IP Configuration Security ACL Queue Strict Priority WRR Weight WRR Bandwidth (% 1 3.3.33% 2 0 1 3.3.33% 2 0 3 0 3 0 3 0 3 1 3 0 3 1 3.3.33% 2 66.67% 3 4 0 4 0 4 1 3 3 1 3 3 1 3 1 1 3 1	Port			_		
VLAN MAC Address Table Spanning Tree Discovery DHCP Multicast IP Configuration Security ACL QoS Image: Control of the security Strict Priority WRR Bandwidth (% 1 3.3.33% 2 0 1 3.3.33% 2 0 3 0 3 0 3 0 3 1 3.3.33% 2 3 0 3 3 1 3.3.33% 2 3 3 3 3 3 3 4 1 3 3 3 1 3 3 1 3 3 1 3 3 1 3 3 3 3 3 3 3 4 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	POE Setting	Queue				
Spanning Tree Discovery DHCP Multicast IP Configuration Security ACL QoS	VLAN		Strict Priority	WRR	Weight	WRR Bandwidth (%)
Discovery DHCP Multicast IP Configuration Security ACL QoS	MAC Address Table	1	0	\bigcirc	1	33.33%
DHCP Multicast IP Configuration Security ACL QoS	Spanning Tree	2	0	\bigcirc	2	66.67%
Multicast 5 5 IP Configuration 5 0 5 Security 6 0 9 ACL 8 0 15 QoS Arabit 15 15	Discovery	3	•	0	3	
IP Configuration Security ACL Qo S	DHCP	4	۲	0	4	
Security 7 13 ACL 8 15 Qo S Actual State Actual State	Multicast	5		0	5	
ACL 8 0 15 QoS	IP Configuration	6	۲	0	9	
ACL 8 O 15 QoS	Security	7		0	13	
QoS	ACL	8	-	0	15	
Apply	QoS		<u> </u>			
	General	Appl	<u>y</u>			
Property	Queue Scheduling					

Description
Queue ID to configure
Set queue to strict priority type
Set queue to Weight round robin type
If the queue type is WRR, set the queue weight for the queue.
Percentage of WRR queue bandwidth

Click the "Apply" button to save your changes settings.

16.3 CoS Mapping

The CoS to Queue table determines the egress queues of the incoming packets based on the 802.1p priority in their VLAN tags. For incoming untagged packets, the 802.1p priority will be the default CoS/802.1p priority assigned to the ingress ports. Use the Queues to CoS table to remark the CoS/802.1p priority for egress traffic from each queue.

V1.0a





Status	CoS to Queue Mapping
Network	
Port	CoS Queue
POE Setting	0 2 🗸
VLAN	1 1 🗸
MAC Address Table	2 3 🗸
Spanning Tree	3 4 🗸
Discovery	4 5 🗸
DHCP	5 6 🗸
Multicast	6 7 🗸
IP Configuration	7 8 🗸
Security	Apply
ACL	
QoS	Queue to CoS Mapping
General	
Property	Queue CoS
Queue Scheduling	1 1 🗸
CoS Mapping	2 0 🗸
DSCP Mapping	3 2 🗸
IP Precedence Mapping	4 3 ₩
Rate Limit	5 4 🗸
Diagnostics	6 5 🗸
Management	7 6 🗸

CoS to Queue Mapping

- **CoS:** CoS value.
- **Queue:** Select queue id for the CoS value.

Click the "Apply" button to save your changes settings.

Queue to CoS Mapping

- Queue: Queue ID.
- **Cos:** Select CoS value for the queue id. \geq

Click the "Apply" button to save your changes settings.



CoS (0 to 7) 7 is highest	Queue(1 to 8) 8 is highest priority	Description
0	2	Background
1	1	Best Effort
2	3	Excellent Effort
3	4	Critical Application LVS phone SIP
4	5	Video
5	6	Voice IP phone default
6	7	Interwork Control LVS phone RTP
7	8	Network Control

16.4 DSCP Mapping

The DSCP to Queue table determines the egress queues of the incoming IP packets based on their DSCP values. The original VLAN Priority Tag (VPT) of the packet is unchanged.

This DSCP values range from 0 through 63, whereas the internal forwarding priority values range from 1 through 8. Any DSCP value within a given range is mapped to the same internal forwarding priority value. These include the CS (Class Selector), AF (Assured Forwarding) and EF (Expedited Forwarding). For example, a packet with a DSCP tag value of 1 can be assigned to the High queue.

Status								
Network	DSCP to	Queue	Mapping					
Port								
POE Setting	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
/LAN	0 [CS0]	1 🗸	16 [CS2]	3 🗸	32 [CS4]	5 🗸	48 [CS6]	7 🗸
AC Address Table	1	1 🗸	17	3 🗸	33	5 🗸	49	7 🗸
anning Tree	2	1 🗸	18 [AF21]	3 🗸	34 [AF41]	5 🗸	50	7 🗸
overy	3	1 🗸	19	3 🗸	35	5 🗸	51	7 🗸
)	4	1 🗸	20 [AF22]	3 🗸	36 [AF42]	5 🗸	52	7 🗸
ast	5	1 🗸	21	3 🗸	37	5 🗸	53	7 🗸
figuration	6	1~	22 [AF23]	3~	38 [AF43]	5 🗸	54	7 🗸
ity	7	1~	23	3 🗸	39	5 🗸	55	7~
	8 [CS1]	2 🗸	24 [CS3]	4~	40 [CS5]	6 🗸	56 [CS7]	8 🗸
	9	2 🗸	25	4 🗸	41	6 🗸	57	8 🗸
eral	10 [AF11]	2 🗸	26 [AF31]	4 ~	42	6 🗸	58	8 🗸
operty	11	2 🗸	27	4 ~	43	6 🗸	59	8 🗸
eue Scheduling S Mapping	12 [AF12]	2 🗸	28 [AF32]	4~	44	6 🗸	60	8 ~
Mapping P Mapping	13	2 🗸	29	4 🗸	45	6 🗸	61	8 🗸

Use the Queues to DSCP page to remark DSCP value for egress traffic from each queue.



DSCP to Queue Mapping

DSCP to (Queue I	Mapping					
DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 🗸	16 [CS2]	3 🗸	32 [CS4]	5 🗸	48 [CS6]	7 🗸
1	1 🗸	17	3 🗸	33	5 🗸	49	7 🗸
2	1 🗸	18 [AF21]	3 🗸	34 [AF41]	5 🗸	50	7 🗸
3	1 🗸	19	3 🗸	35	5 🗸	51	7 🗸
4	1 🗸	20 [AF22]	3 🗸	36 [AF42]	5 🗸	52	7 🗸
5	1 🗸	21	3 🗸	37	5 🗸	53	7 🗸
6	1 🗸	22 [AF23]	3 🗸	38 [AF43]	5 🗸	54	7 🗸
7	1 🗸	23	3 🗸	39	5 🗸	55	7 🗸
8 [CS1]	2 🗸	24 [CS3]	4 🗸	40 [CS5]	6 🗸	56 [CS7]	8 🗸
9	2 🗸	25	4 🗸	41	6 🗸	57	8 🗸
10 [AF11]	2 🗸	26 [AF31]	4 🗸	42	6 🗸	58	8 🗸
11	2 🗸	27	4 🗸	43	6 🗸	59	8 🗸
12 [AF12]	2 🗸	28 [AF32]	4 🗸	44	6 🗸	60	8 🗸
13	2 🗸	29	4 🗸	45	6 🗸	61	8 🗸
14 [AF13]	2 🗸	30 [AF33]	4 🗸	46 [EF]	6 🗸	62	8 🗸
15	2 🗸	31	4 🗸	47	6 🗸	63	8 🗸
Apply							

- \geq DSCP: DSCP value.
- \geq **Queue:** Select queue id for DSCP value.

Click the "Apply" button to save your changes settings.

Queue to DSCP Mapping





Queue	DSCP
1	0 [CS0] 🗸
2	8 [CS1] 🗸
3	16 [CS2] 🗸
4	24 [CS3] 🗸
5	32 [CS4] 🗸
6	40 [CS5] 🗸
7	48 [CS6] 🗸
8	56 [CS7] 🗸

 \geq Queue: DSCP value.

DSCP: Select DSCP value for queue id. \geq

Click the "Apply" button to save your changes settings.

16.5 IP Precedence to Queue Mapping

This page allow user to configure IP Precedence to Queue mapping and Queue to IP Precedence mapping, The IP Precedence standard uses the first 3 bits of the ToS byte to mark packets with 8 levels of priority, numbered 0-7, with 0 being the lowest priority and 7 the highest. Because IP Precedence and ToS use different bits in the ToS byte to mark the priority of a packet, they can co-exist in the same packet header without interfering with each other.





ecedence to Queue Mapping 0 1 • 1 2 • 2 3 • 3 4 • 4 5 • 5 6 • 6 7 • 7 8 • pply e to IP Precedence Mapping
0 1 v 1 2 v 2 3 v 3 4 v 4 5 v 5 6 v 6 7 v 7 8 v
0 1 v 1 2 v 2 3 v 3 4 v 4 5 v 5 6 v 6 7 v 7 8 v
1 $2 \checkmark$ 2 $3 \checkmark$ 3 $4 \checkmark$ 4 $5 \checkmark$ 5 $6 \checkmark$ 6 $7 \checkmark$ 7 $8 \checkmark$ apply
2 3 v 3 4 v 4 5 v 5 6 v 6 7 v 7 8 v
3 4 v 4 5 v 5 6 v 6 7 v 7 8 v
4 5 × 5 6 × 6 7 × 7 8 ×
5 6 ~ 6 7 ~ 7 8 ~
6 7 v 7 8 v
7 8 🗸
oply
e to IP Precedence Mapping
e IP Precedence
2 1 •
3 2 🗸
4 3 •
5 4 🗸
6 5 v
7 6 v

IP Precedence to Queue mapping

- > IP Precedence: IP Precedence value.
- \geq **Queue:** Queue value which IP Precedence is mapped.

Click the "Apply" button to save your changes settings.

Queue to IP Precedence mapping

- **Queue:** Queue ID.
- **IP Precedence:** IP Precedence value which queue is mapped. \geq

Click the "Apply" button to save your changes settings.





16.6 Rate Limit

This page allow user to configure ingress port rate limit and egress port rate limit. The ingress rate limit is the number of bits per second that can be received from the ingress interface. Excess bandwidth above this limit is discarded.

Ingress / Egress Port 16.6.1

The rate limiting function can be configured to limit of Ingress/Egress traffic on a particular interface.

Administrator can set Ingress/Egress rate limiting in Ports. The usage rate is 16 to 10000000 Kbps

QoS → Rate Limit → Ingr	ess / Eg	ress Po	ort				
✓ Status							
* Network	Ing	ress / E	gress	Port Tab	le		
₽ Port							
POE Setting							
¥ VLAN				In	gress	E	gress
MAC Address Table		Entry	Port	State	Rate (Kbps)	State	Rate (Kbps)
 Spanning Tree 		1	GE1	Enabled	102400	Enabled	102400
Solution Discovery		2	GE2	Enabled	102400	Enabled	102400
♥ DHCP		3	GE3	Disabled	102400	Disabled	102400
 Multicast 		-			102.400		402400
 IP Configuration 		4	GE4	Enabled	102400	Enabled	102400
✓ Security		5	GE5	Enabled	102400	Enabled	102400
* ACL		6	GE6	Disabled		Disabled	
– QoS		7	GE7	Disabled		Disabled	
a General		8	GE8	Disabled		Disabled	
Property		9	GE9	Disabled		Disabled	
Queue Scheduling		10	GE10	Disabled		Disabled	
CoS Mapping DSCP Mapping		11	GE11	Disabled		Disabled	
IP Precedence Mapping		12	GE12	Disabled		Disabled	
		13	GE13	Disabled		Disabled	
Ingress / Egress Port		14	GE14	Disabled		Disabled	
Egress Queue		15	GE15	Disabled		Disabled	

Field	Description
Port	Port name.
Trust	Port ingress rate limit state:Enabled: To enabled Ingress rate limit function.





	Disabled: To disabled the Ingress rate limit function.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
Ingress (Rate)	Port ingress rate limit value if ingress rate state is enabled.
IP Precedence	IP Precedence value which queue is mapped.
Trust	 Port egress rate limit state: Enabled: To enabled Egress rate limit function. Disabled: To disabled Egress rate limit function.
Egress (Rate)	Port egress rate limit value if egress rate state is enabled.

Port	GE1-GE2,GE4-GE5		
Ingrass	Enable		
Ingress	102400	Kbps (16 - 1000000)	
-	Enable		
Egress	102400	Kbps (16 - 1000000)	

- **Port:** Select the checkbox for port list. \geq
- Ingress : Set checkbox to enable/disable ingress rate limit. If ingress rate limit is enabled, rate \geq limit value need to be assigned, The control Range is "16-10000000 Kbps".
- Ingress : Set checkbox to enable/disable egress rate limit. If egress rate limit is enabled, rate \geq limit value need to be assigned, The control Range is "16-10000000 Kbps".
- \geq Ingress : Set checkbox to enable/disable ingre

Click the "Apply" button to save your changes or "Close" the button to close settings.

16.6.2 **Egress Queue**

The Egress Queue function can be configured priority Queue by QoS. Egress rate limiting is performed by shaping the output load. Administrator can set Ingress Queue by limiting QoS . The usage rate is 16 to 1000000 Kbps, Please Click "Edit" button to set the Egress Queue Port menu.





QoS → Rate Limit → Egress Queue

ork	Egre	ess Qu	eue Ta	able								
	_											
				Qu	Queue 1		Queue 2		Queue 3		Queue 4	
		Entry	Port	State	CIR (Kbps)							
		1	GE1	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		
		2	GE2	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		
		3	GE3	Disabled	01200	Disabled	01200	Disabled	02400	Disabled		
		4	GE4	Disabled		Disabled		Disabled		Disabled		
	H	5	GE5	Disabled		Disabled		Disabled		Disabled		
			GE6	Disabled		Disabled		Disabled		Disabled		
		6										
		7	GE7	Disabled		Disabled		Disabled		Disabled		
		8	GE8	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		
		9	GE9	Disabled		Disabled		Disabled		Disabled		
g		10	GE10	Disabled		Disabled		Disabled		Disabled		
		11	GE11	Enabled	51200	Enabled	51200	Enabled	62496	Disabled		
g Mapping		12	GE12	Disabled		Disabled		Disabled		Disabled		
ico mapping		13	GE13	Disabled		Disabled		Disabled		Disabled		
ess Port		14	GE14	Disabled		Disabled		Disabled		Disabled		
		15	GE15	Disabled		Disabled		Disabled		Disabled		

Egress Queue Table

_																		
	Entry	Port	્રા	ueue 1	િવા	Jeue 2	Qu	ieue 3	Qı	Jeue 4	Qu	ieue 5	Qı	ieue 6	Qu	ieue 7	Qu	eue 8
	cnuy	Poit	State	CIR (Kbps)														
	1	GE1	Enabled	51200	Enabled	51200	Enabled	62496	Disabled									
	2	GE2	Enabled	51200	Enabled	51200	Enabled	62496	Disabled									
	3	GE3	Disabled															
	4	GE4	Disabled															
	5	GE5	Disabled															
	6	GE6	Disabled															
	7	GE7	Disabled															
	8	GE8	Enabled	51200	Enabled	51200	Enabled	62496	Disabled									
	9	GE9	Disabled															

Field	Description
Port	Interface of port number.
Quere 1 (State)	Port egress queue 1 rate limit state
Queue 1 (State)	 Enabled: Egress queue rate limit is enabled.
	Disabled: Egress queue rate limit is disabled.
Queue 1 (CIR)	Queue 1 egress committed information rate.
Queue 2 (State)	Port egress queue 2 rate limit state.
Queue 2 (State)	 Enabled: Egress queue rate limit is enabled.
	Disabled: Egress queue rate limit is disabled.
Queue 2 (CIR)	Queue 2 egress committed information rate.
	Port egress queue 3 rate limit state.
Queue 3 (State)	 Enabled: Egress queue rate limit is enabled.
	Disabled: Egress queue rate limit is disabled.





Queue 3 egress committed information rate.					
Port egress queue 4 rate limit state.					
 Enabled: Egress queue rate limit is enabled. 					
Disabled: Egress queue rate limit is disabled.					
Queue 4 egress committed information rate.					
Port egress queue 5 rate limit state.					
• Enabled: Egress queue rate limit is enabled.					
Disabled: Egress queue rate limit is disabled.					
Queue 5 egress committed information rate.					
Port egress queue 6 rate limit state.					
 Enabled: Egress queue rate limit is enabled. 					
Disabled: Egress queue rate limit is disabled					
Queue 6 egress committed information rate.					
Port egress queue 7 rate limit state.					
 Enabled: Egress queue rate limit is enabled. 					
• Disabled: Egress queue rate limit is disabled.					

Port	GE1-GE2,GE8,GE1	1	
	Enable		
Queue 1	51200	Kbps (16 - 1000000)	
	Enable		
Queue 2			
	51200	Kbps (16 - 1000000)	
	Enable		
Queue 3	1128000	Kbps (16 - 10000000)	
	1120000	Kups (10 - 1000000)	
0	Enable		
Queue 4	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 5	1000000	Kbps (16 - 10000000)	
	Enable		
Queue 6			
	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 7	4000000		
	1000000	Kbps (16 - 1000000)	
	Enable		
Queue 8	1000000	Kbps (16 - 1000000)	

Set checkbox to enable/disable ingress priority queue 1 to~ queue 8 level , The control range is "16-1000000 Kbps"





- \geq **Port:** Select one or multiple ports for the configure.
- \geq Queue 1: Set checkbox to enable/disable egress queue 1 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq Queue 2: Set checkbox to enable/disable egress queue 2 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq **Queue 3:** Set checkbox to enable/disable egress queue 3 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq Queue 4: Set checkbox to enable/disable egress queue 4 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq **Queue 5:** Set checkbox to enable/disable egress queue 5 rate limit.
 - **Enable:** If egress rate limit is enabled, rate limit value need to be assigned.
- Queue 6: Set checkbox to enable/disable egress queue 6 rate limit. \geq
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq **Queue 7:** Set checkbox to enable/disable egress queue 7 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.
- \geq Queue 8: Set checkbox to enable/disable egress queue 8 rate limit.
 - Enable: If egress rate limit is enabled, rate limit value need to be assigned.

Click the "Apply" button to save your changes or "Close" the button to close settings.

Diagnostics 17.

17.1 Logging

17.1.1 Property

This function support log message includes Console / RAM / Flash message send to remote log server. Administrator can enable or disable this function. Use the Diagnostics pages to configure settings for the switch diagnostics feature or operating diagnostic utilities.





Diagnostics → Logging → Property	
* Status	
* Network State	e 🔽 Enable
* Port	
* POE Setting Aggregation	1 🔽 Enable
* VLAN Aging Time	B 300 Sec (15 - 3600, default 300)
MAC Address Table	
Spanning Tree Console Logg	jing
* Discovery State	
* DHCP	
* Multicast Minimur	L
IP Configuration Severity	Note: Emergency, Alert, Critical, Error, Warning, Notice
* Security	
* ACL RAM Logging	
¥ QoS State	e 🔽 Enable
– Diagnostics Minimur	Notice 🗸
Logging Severity	L

- \geq State: When the logging service is enabled, logging configuration of each destination rule can be individually configured. If the logging service is disabled, no messages will be sent to these destinations.
 - **Enable:** Enable/Disable the global logging services.
- \geq Aggregation:
 - Enable: Enable/Disable the aggregation services.
 - Aging: 15~3600 Second. The default is 300 second.
- \geq **Console Logging:**
 - **State:** Enable/Disable the Console Logging services.
 - Minimum Severity: The minimum severity for the Console Logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.
- \geq **RAM Loggong:**
 - **State:** Enable/Disable the RAM Loggong services.
 - **Minimum Severity:** The minimum severity for the RAM logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.
- \geq Flash Loggong:
 - State: Enable/Disable the Flash Loggong services.
 - Minimum Severity: The minimum severity for the flash logging. Including selection of events such as Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug, etc.





• Emergency—System is not usable. Note • Warning—System warning has occurred. • Notice—System is functioning properly, but a system notice has occurred.

Click the "Apply" button to save your changes settings.

17.1.2 **Remote Server**

Use the Remote Log Servers page to define the remote SYSLOG servers where log messages are sent (using the SYSLOG protocol). For each server, you can configure the severity of the messages that it receives, Setting "add" and "Edit" and "Delete" for this function management.

Diagnostics → Logging						
Network	Ren	note Se	erver Table			
⊭ Port						
POE Setting						Q,
¥ VLAN		1				Minimum
MAC Address Table		Entry	Server Address	Server Port	Facility	Severity
Spanning Tree		1	192,168,2,99	514	Local 7	Notice
Discovery		2	192.168.2.101	514	Local 7	Warning
⊭ DHCP		-	102.100.2.101	514	Locarr	manning
Multicast		Add	Edit	Delete		
IP Configuration	_					
⊭ Security						
# ACL						
¥ QoS						
- Diagnostics						
Logging						
Property						
Remote Server						





Field	Description					
Server Address	The IP address of the remote logging server.					
Server Ports	The port number of the remote logging server.					
Facility	The facility of the logging messages. It can be one of the following values: local0, local1, local2, local3, local4, local5, local6, and I7.					
	The minimum severity.					
	Emergence: System is not usable.					
	 Alert: Immediate action is needed. 					
	 Critical: System is in the critical condition. 					
	• Error: System is in error condition.					
Minimum Severity	Warning: System warning has occurred.					
	 Notice: System is functioning properly, but a system notice has 					
	occurred.					
	Informational: Device information.					
	 Debug: Provides detailed information about an event. 					

Address Type	 ○ Hostname ● IPv4 ○ IPv6
Server Address	192.168.2.101
Server Port	514 (1 - 65535, default 514)
Facility	Local 7 🗸
Minimum Severity	Warning Note: Emergency, Alert, Critical, Error, Warning

- \triangleright Address Type: Administrator can select use Hostname or IPv4/6 connection remote log server.
- \geq Server Address: Enter the IP address of the server.
- \geq Server Port: Enter service port to which the log messages are sent.
- \succ Facility: Select a facility from which system logs are sent to the remote server. Only one facility can be assigned to a server.
- Minimum Severity: Select the minimum level of system log messages to be sent to the server. \geq
 - Emergence: System is not usable.

V1.0a





- Alert: Immediate action is needed.
- Critical: System is in the critical condition.
- Error: System is in error condition.
- Warning: System warning has occurred.
- Notice: System is functioning properly, but a system notice has occurred.
- Informational: Device information.
- Debug: Provides detailed information about an event..

Click the "Apply" button to save your changes or "Close" the button to close settings.

17.2 Mirroring

Mirroring function can mirror Rx/Tx traffic, Packet can mirror to destination port and for analysis.

Diagnostics 🏽 Mirroring	-					
⊌ Status						
Network	Mirr	oring Table	е			
⊌ Port						
POE Setting					C	2
* VLAN		Session ID	State	Monitor Port	Ingress Port	Egress Port
MAC Address Table	0	1	Disabled			
Spanning Tree	0	2	Enabled	GE2 (Normal*)	GE3	GE3-GE4
 Discovery 						
* DHCP	0	3	Disabled			
 Multicast 	0	4	Disabled			
 IP Configuration 		Edit				
 Security 						
* ACL					,	
¥ QoS		*" Allow the mo	onitor port to	send or receive r	ormal packets	
– Diagnostics						
 Logging Property Remote Server Mirroring 						

Field	Description
Session ID	Select mirror session ID
	Select mirror session state : port-base mirror or disable
State	Enabled: Enable port based mirror
	• Disabled: Disable mirror.





Monitor Port	Select mirror session monitor port, and select whether normal packet could be sent or received by monitor port.
Ingress port	Select mirror session source rx ports
Egress ports	Select mirror session source tx ports

Click the "Edit" button to edit your settings.

Edit Mirroring		
Session ID	2	
State	Enable	
	GE2 V	
Monitor Port		
	Send or Receive N	lormal Packet
	Available Port	Selected Port
	GE1	GE3
	GE2	GES A
Ingress Port	GE4	
	GE5 GE6	
	GE7 <	
	GE8 GE9 •	_
	Available Port	Selected Port
	GE1	GE3
	GE2 GE5	GE4
Egress Port	GE5 GE6	
	GE7	
	GE8 GE9	
	GE9 GE10 -	
Apply]	Close	

- \geq Session ID: Display selected mirror session ID.
- \geq State:
 - **Enable:** Enable/Disable the mirroring function.
- \geq Mirroring Port: Administrator can choose a mirroring Port.
- \geq Ingress Port: Administrator can choose mirrored ports for ingress.
- \succ Egress Port: Administrator can choose mirrored ports for egress

Click the "Apply" button to save your changes or "Close" the button to close settings.





17.3 Ping

The Ping utility tests if a remote host can be reached and measures the round-trip time for packets sent from the device to a destination device.

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response, sometimes called a pong. It measures the round-trip time and records any packet loss, Administrators can use this ping function to check connected device whether is active. This ping function support IPv4 and IPv6 protocol.

Diagnostics >> Ping		
* Network		Hostname
✤ Port	Address Type	
POE Setting		○ IPv6
* VLAN	Server Address	162.159.200.1
 MAC Address Table 	Count	4 (1 - 32)
Spanning Tree	Count	
* Discovery	[Disc.] Ob	
* DHCP	Ping Sto	<u>op</u>
 Multicast 	Ping Result	
 IP Configuration 		
 Security 	Packet Status	
* ACL	Status	Success.
¥ QoS	Transmit Packet	
- Diagnostics		
Eogging	Receive Packet	4
Mirroring	Packet Lost	0 %
Ping		
Traceroute Copper Test	Round Trip Time	
Fiber Module	Min	0 ms
© UDLD	Max	10 ms
 Management 	Average	2 ms

- \geq Address Type: Specify the address type to "Hostname", "IPv6", or "IPv4".
- Server Address: Specify the Hostname/IPv4/IPv6 address for the remote logging server. \geq
- \geq **Count:** Specify the numbers of each ICMP ping request.

Click the "Ping" button to ping result appears.





Field	Description			
	Displays whether the ping succeeded or failed.			
	 Status: Displays the ping result status of "Success" or "Ping failed 			
Packet Status	(timeout)".			
Packet Status	 Transmit Packet: Number of packets sent by ping. 			
	 Receive Packet: Number of packets received by ping. 			
	 Packet Lost: Percentage of packets lost in ping process. 			
	Displays the ping round trip time.			
	• Min: Shortest time for packet to return.			
Round Trip Time	• Max: Longest time for packet to return.			
	 Average: Average time for packet to return 			

17.4 Traceroute

Traceroute discovers the IP routes along which packets were forwarded by sending an IP packet to the target host and back to the switch. The Traceroute page displays each hop between the switch and a target host and the round-trip time to each hop.

Diagnostics 🇃 Traceroute						
* Status						
* Network	Hostname					
✤ Port	Address Type					
 POE Setting 	Server Address 162,159,200,1					
* VLAN	Server Address [102.159.200.1					
MAC Address Table	User Defined					
 Spanning Tree 	Time to Live 30 (2 - 255, default 30)					
Discovery						
* DHCP	Apply Stop					
 Multicast 						
 IP Configuration 	Traceroute Result					
✤ Security						
* ACL	traceroute to 162.159.200.1 (162.159.200.1), 30 hops max, 38 byte packets					
¥ QoS	1 192.168.101.254 (192.168.101.254) 0.000 ms 0.000 ms 0.000 ms					
- Diagnostics	2 60.248.167.254 (60.248.167.254) 10.000 ms 10.000 ms 10.000 ms 3 168.95.82.206 (168.95.82.206) 0.000 ms 0.000 ms 10.000 ms					
S Logging	4 220.128.2.226 (220.128.2.226) 0.000 ms 10.000 ms 0.000 ms					
Mirroring	5 220.128.1.125 (220.128.1.125) 10.000 ms 10.000 ms 10.000 ms 6 203.75.230.125 (203.75.230.125) 10.000 ms 10.000 ms 10.000 ms					
Ping	7 162.159.200.1 (162.159.200.1) 10.000 ms 10.000 ms 10.000 ms					
Traceroute	Trace complete					
Copper Test						
Fiber Module						
© UDLD						



- Address Type: Specify the address type to "Hostname", or "IPv4". \geq
- Server Address: Specify the Hostname/IPv4 address for the remote logging server. \succ
- \geq Time to Live :Enter the maximum number of hops that Traceroute permits. This is used to prevent a case where the sent frame gets into an endless loop. The Traceroute command terminates when the destination is reached or when this value is reached. To use the default value (30), select Use Default.

Click the "Apply" button to Traceroute result appears.

17.5 Copper Test

Administrator can use this function check port Result whether is working, if working then display it.

Diagnostics → Copper Test	
Network	Port GE28 V
✤ Port	
 POE Setting 	Copper Test
* VLAN	Copper rest
MAC Address Table	
 Spanning Tree 	Copper Test Result
 Discovery 	
* DHCP	Cable Status
 Multicast 	Port GE28
 IP Configuration 	
 Security 	Result Open Cable
* ACL	Length 0.87 M
¥ QoS	
– Diagnostics	
 Logging Mirroring Ping Traceroute Copper Test 	

Field	Description
Port	Specify the interface for the copper test.

Click the "Copper Test" button to Copper Test result appears.



Cable Status

Field	Description
Port	The interface for the copper test.
	The status of copper test. It include:
	OK: Correctly terminated pair.
	Short Cable: Shorted pair.
Result	• Open Cable: Open pair, no link partner.
nesure	 Impedance Mismatch: Terminating impedance is not in the reference
	range.
	• Line Drive:
Length	Distance in meter from the port to the location on the cable where the fault was discovered.

17.6 Fiber Module

Display Fiber module messenger. The Optical Module Status page displays the operational information reported by the Small Form-factor Pluggable (SFP) transceiver. Some information may not be available for SFPs without the supports of digital diagnostic monitoring standard SFF-8472.

Diagnostics 🗃 Fiber Module	e
Network	Fiber Module Table
✤ Port	
✤ POE Setting	Q,
* VLAN	Port Temperature (C) Voltage (V) Current (mA) Output Power (mW) Input Power (mW) OE Present Loss of Signal
MAC Address Table	0 results found.
 Spanning Tree 	
 Discovery 	Refresh Detail
* DHCP	
 Multicast 	
 IP Configuration 	
✓ Security	
* ACL	
¥ QoS	
– Diagnostics	
S Logging	
Mirroring	
Ping	
Traceroute	
Copper Test	
Fiber Module	





Field	Description				
Port	Interface or port number.				
Temperature	Internally measured transceiver temperature.				
Voltage	Internally measured supply voltage.				
Current	Measured TX bias current.				
Output Power	Measured TX output power in mill watts.				
Input Power	Measured RX received power in mill watts.				
Transmitter Fault	State of TX fault.				
OE Present	Indicate transceiver has achieved power up and data is ready.				
Loss of Signal	Loss of signal.				
Refresh	Refresh the page.				
Detail	The detail information on the specified port.				

Click the "Refresh" button to refresh this page or click the "*Detail*" button to check detail information.

17.7 UDLD

Uni-Directional Link Detection (UDLD) monitors a link between two devices and brings the ports on both ends of the link down if the link goes down at any point between the two devices, Use the UDLD pages to configure settings of UDLD function.

17.7.1 Property

This page allow user to configure global and per interface settings of UDLD.





01-1	Property						
Status							
Network		Messag	e Time	15	Sec	(1 - 90, default 15)	
≠ Port		messag	e mile			(1 50, doidait 15)	
POE Setting			1				
≠ VLAN		pply	ļ				
MAC Address Table							
Spanning Tree	Port	Settin	g Tabl	e			
Discovery							
≠ DHCP							
Multicast		Entry	Port	Mode	Bidirectional State	Operational Status	Neighb
IP Configuration		1	GE1	Normal	Unknown	Link down	0
Security		2	GE2	Normal	Unknown	Link down	0
ACL		3	GE3	Disabled	Unknown		0
QoS		4	GE4	Disabled	Unknown		0
– Diagnostics		5	GE5	Disabled	Unknown		0
S Logging		6	GE6	Disabled	Unknown		0
Mirroring				Disabled			-
Ping		7	GE7		Unknown		0
Traceroute Copper Test		8	GE8	Disabled	Unknown		0
Fiber Module		9	GE9	Disabled	Unknown		0
♦ UDLD		10	GE10	Disabled	Unknown		0
Property		11	GE11	Disabled	Unknown		0
Neighbor		12	GE12	Disabled	Unknown		0

Message Time: To use the UDLD protocol all connected switches and interfaces have to be configured for it. A UDLD configured switch sends UDLD advertisements, "hello" packets to its neighbors and expects to receive one in the designated hold time (the default hold time is 15mins). If this doesn't happen the UDLD disables the unresponsive interface..

Click the "Apply" button to save your changes settings.

Field	Description
Port	Display port ID of entry.
Mode	Display UDLD running mode of interface.
Bidirectional State	Display bidirectional state of interface.
Operational Status	Display operational status of interface

V1.0a







Neighbor

Display the number of neighbor of interface

Edit Port Setting	
Port	GE1-GE2
Mode	 Disabled Normal Aggressive
Apply	Close

- **Port:** Select one or multiple ports for the configure.
- > Mode: Select UDLD running mode of interface.
 - **Disabled:** Disable UDLD function.
 - Normal: Running on normal mode that port goes to Link Up One phase after last neighbor ages out.
 - Aggressive: Running on aggressive mode that port goes to Re-Establish phase after last neighbor ages out.

Click the "Apply" button to save your changes or "Close" the button to close settings.

17.7.2 Neighbor

Each switch port that is configured for UDLD exchanges UDLD protocol packets that include information about the port's device and port ID, and the port also sends the same device and port ID information that it knows about its connected neighbor.

Because of this, a port should receive its own device and port ID information from its neighbor if the link is bi-directional. If a port does not receive information about its own device and port ID from its neighbor, the link is considered to be unidirectional.

This can occur when the link is up on both sides, but one side is not receiving packets, or when wiring mistakes occur, causing the transmit and receive wires to not be connected to the same ports on both ends of a link.





Diagnostics ⇒ UDLD ⇒ No	eighbor							
✓ Status								
Network	Neighl	bor Table						
⊭ Port								
POE Setting								Q,
\$ VLAN		Expiration					Message	Timeout
MAC Address Table	Entry	Time	Current Neighbor State	Device ID	Device Name	Port ID	Interval	Interval
 Spanning Tree 					0 results found.			
Discovery					o roculto roculta.			
* DHCP	Refre	esh						
 Multicast 								
 IP Configuration 								
Security								
¥ ACL								
¥ QoS								
– Diagnostics								
 Logging Mirroring Ping Traceroute Copper Test Fiber Module UDLD Property Neighbor 								

Field	Description
Entry	Display entry index.
Expiration Time	Display expiration time before age out.
Current Neighbor State	Display neighbor current state
Device ID	Display neighbor device ID.
Device Name	Display neighbor device name.
Port ID	Display neighbor port ID that connected.
Message Interval	Display neighbor message interval.
Timeout Interval	Display neighbor timeout interval





18. Management

18.1 User Account

The default username/password is root/default. Administrator can modify login password or create new username / password and defined Privilege, Setting "add" and "Edit" and "Delete" function for this management.

Management 🗩 User Accour	nt
* Status	
 Network 	User Account
✤ Port	
POE Setting	Showing All entries Showing 1 to 3 of 3
¥ VLAN	Username Privilege
MAC Address Table	root Admin
 Spanning Tree 	mis Admin
* Discovery	number1 User
* DHCP	
* Multicast	Add Edit Delete
IP Configuration	
Security	
* ACL	
¥ QoS	
Diagnostics	
- Management	
User Account Firmware	
© Configuration	
© SNMP	
© RMON	

Field	Description
Username	User name of the account



	Display privilege level for new account.
_	• Admin: Allow to change switch settings. Privilege value equals to 15.

Privilege

• User: See switch settings only. Not allow to change it. Privilege level equals to 1.

Add User Account	
Username	
Password	
Confirm Password	
Privilege	Admin User
Apply Close	

- \triangleright Username: User name of the account.
- Password: Set password of the account. \geq
- Confirm Password: Set the same password of the account as in "Password" field. \geq
- \geq Privilege: Select privilege level for new account.
 - Admin: Allow to change switch settings. Privilege value equals to 15.
 - User: See switch settings only. Not allow to change it. Privilege level equals to 1.

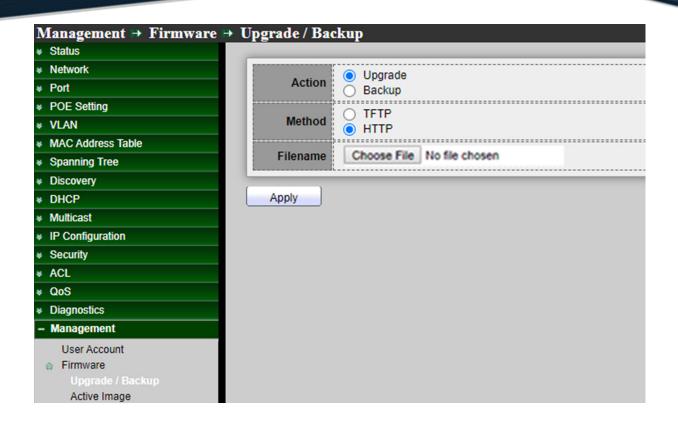
Click the "Apply" button to save your changes or "Close" the button to close settings.

18.2 Firmware

18.2.1 **Upgrade / Backup**

Administrator can upgrade or backup firmware, method can choose use TFTP or HTTP protocol. If choose backup then administrator can choose firmware image to backup.





- \succ Action: Firmware operations.
 - Upgrade: Upgrade firmware from remote host to DUT.
 - Backup: Backup firmware image from DUT to remote host.
- \succ Method: Firmware upgrade / backup method.
 - **TFTP:** Using TFTP to upgrade/backup firmware.
 - **HTTP:** Using WEB browser to upgrade/backup firmware.
- \geq Filename: Use browser to upgrade firmware, you should select firmware image file on your host PC.

Click the "Apply" button to save your changes settings.

Action	O Upgrade Backup
Method	● TFTP ○ HTTP
Firmware	Image
Address Type	 Hostname IPv4 IPv6
Server Address	
Filename	
Apply	



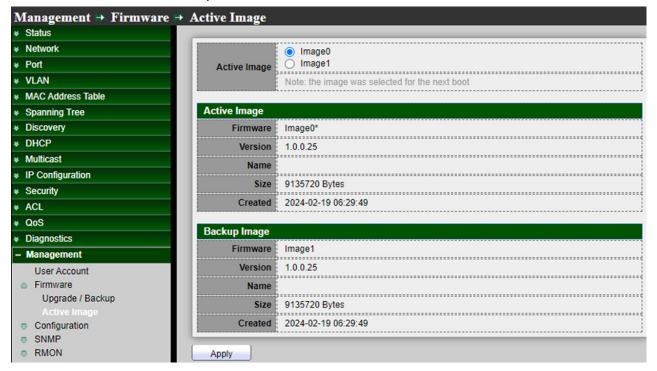


- Action: Firmware operations. \geq
 - Upgrade: Upgrade firmware from remote host to DUT.
 - Backup: Backup firmware image from DUT to remote host.
- \triangleright Method: Firmware upgrade / backup method.
 - **TFTP:** Using TFTP to upgrade/backup firmware.
 - **HTTP:** Using WEB browser to upgrade/backup firmware.
- \triangleright Firmware: Firmware image in default flash.
- \geq Address Type: Specify TFTP server address type
 - Hostname: Use domain name as server address.
 - **IPv4:** Use IPv4 as server address.
 - IPv6: Use IPv6 as server address
- \geq Server Address: Specify TFTP server address.
- \geq Filename: Firmware image file name on remote TFTP server.

Click the "Apply" button to save your changes settings.

18.2.2 **Active Image**

This page allows user to select firmware image on next booting and show firmware information on both flash partitions, If the Switch has upload multiple firmware in system then administrator can choose a firmware to do system default start.



V1.0a





- Active Image: Select firmware image to use on next booting. \succ
 - Image0: Select the flash partition 0 for Firmware image0 to active.
 - Image1: Select the flash partition 1 for Firmware image1 to active.

Field	Description			
Active Image	• Firmware: Firmware image.			
	Version: Firmware version			
	Name: Firmware name.			
	Size: Firmware image size.			
	Created: Firmware image created date.			
	Firmware: Firmware image.			
Backup	Version: Firmware version			
Image	Name: Firmware name.			
	• Size: Firmware image size.			
	Created: Firmware image created date.			

Click the "Apply" button to save your changes settings.

18.3 Configuration

Upgrade / Backup 18.3.1

Administrator can backup system configuration file to PC or upload configuration file to Switch system, This page allow user to upgrade or backup firmware image through HTTP or TFTP server.





Management → Configurat	tion → Upgrade / E	Sackup
v Network		Upgrade
⊭ Port	Action	O Backup
POE Setting		○ TFTP
¥ VLAN	Method	HTTP
MAC Address Table		Running Configuration
 Spanning Tree 		Startup Configuration
 Discovery 	Configuration	 Backup Configuration
* DHCP		C RAM Log
 Multicast 		
IP Configuration	Filename	│選擇檔案│未選擇任何檔案
 Security 		
* ACL	Apply	
¥ QoS		
 Diagnostics 		
– Management		
User Account		
Firmware		
Configuration		
Upgrade / Backup		
Save Configuration SNMP		
© SNMP © RMON		

Upgrade Configuration

- \geq Action: Configuration operations.
 - Upgrade: Upgrade firmware from remote host to DUT.
 - Backup: Backup firmware image from DUT to remote host.
- \geq Method: Configuration upgrade method.
 - **TFTP:** Using TFTP to upgrade firmware.
 - **HTTP:** Using WEB browser to upgrade firmware.
- \geq Configuration: Configuration Type.
 - Running Configuration: Merge to current running configuration file.
 - Startup Configuration: Replace startup configuration file.
 - Backup Configuration: Replace backup configuration file.
- \geq Address Type: Specify TFTP server address type
 - Hostname: Use domain name as server address.
 - **IPv4:** Use IPv4 as server address.
 - **IPv6:** Use IPv6 as server address
- Server Address: Specify TFTP server address. \geq
- \geq Filename: Configuration file name on remote TFTP server.

Click the "Apply" button to save your changes settings.

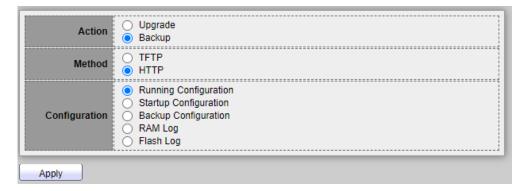
+(886) 2-8911-6160







Backup Configuration



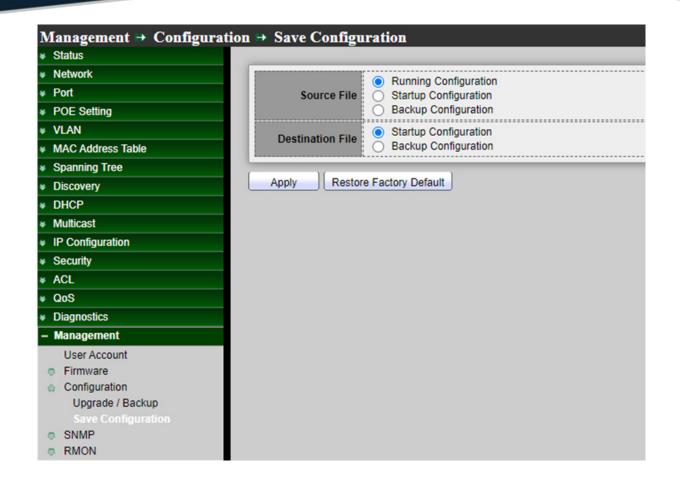
- \geq Action: Configuration operations.
 - Upgrade: Upgrade firmware from remote host to DUT.
 - Backup: Backup firmware image from DUT to remote host.
- Method: Configuration backup method. \geq
 - **TFTP:** Using TFTP to backup firmware.
 - **HTTP:** Using WEB browser to backup firmware.
- Configuration: Configuration Type. \geq
 - Running Configuration: Backup running configuration file.
 - Startup Configuration: Backup start configuration file.
 - Backup Configuration: Backup backup configuration file.
 - RAM Log: Backup log file stored in RAM.
 - Flash Log: Backup log files store in Flash.

Click the "Apply" button to save your changes settings.

18.3.2 **Save Configuration**

When administrator to click Apply on any window, changes that you made to the switch configuration settings are stored only in the Running Configuration. To preserve the parameters in the Running Configuration, the Running Configuration must be copied to another configuration type or saved as a file on another device, This page allow user to manage configuration file saved on DUT and click "Restore Factory Default" button to restore factory defaults.





- \geq Source File: Source file types
 - Running Configuration: Copy running configuration file to destination.
 - Startup Configuration: Copy startup configuration file to destination.
 - Backup Configuration: Copy backup configuration file to destination.
- Destination File: Destination file types. \triangleright
 - **Startup Configuration:** Save file as startup configuration.
 - Backup Configuration: Save file as backup configuration.

Click the "Apply" button to save your changes or Chick "Restore Factory Default" the button to back to factory default setting.





18.4 SNMP

The SNMP supports SNMP v1, v2, and v3. It also reports system events to trap receivers using the traps defined in the Management Information Base (MIB) that it supports.

18.4.1 View

A view is a user-defined label for a collection of MIB tree subtrees. Each subtree ID is defined by the OID of the root of the relevant subtrees. You can either use well-known names to specify the root of the desired subtree or enter an OID. Setting **"add"** or **"Delete"** to management.

Management ↦ SNMP ↦ Vi	iew			
* Status				
Network	View Table	e		
∗ Port				
✤ POE Setting	Showing All	✓ entries	Showing 1 to 1 of 1 entries	Q
* VLAN	View	OID Subtree	Туре	
MAC Address Table	all	.1	Included	
 Spanning Tree 			First	Previ
Discovery	Add	Delete		Flevi
* DHCP	Add	Delete		
⊭ Multicast				
 IP Configuration 				
✓ Security				
* ACL				
⊭ QoS				
 Diagnostics 				
– Management				
User Account				
Firmware				
 Configuration SNMP 				
SNMP View				
Group				
Community				
User				
Engine ID				
Trap Event				
Notification				
© RMON				

Field	Description
View	The SNMP view name. Its maximum length is 30 characters.





Subtree OID	Specify the ASN.1 subtree object identifier (OID) to be included or excluded from the SNMP view.		
View Type	Include or exclude the selected MIBs in the view.		

Add View	
View	
OID Subtree	
Туре	 Included Excluded
Apply	Close

- **View:** Enter a unique view name.
- \succ Object Subtree: Select User Defined to manually define an OID, or select an existing OID from the list. All descendent of this node will be included or excluded in the view.
- \triangleright Type:

Include: Check to include the selected MIBs in this view. Excluded: Check to Excluded the selected MIBs in this view.

18.4.2 Group

In SNMPv1 and SNMPv2, a community string is sent along with the SNMP frames. The community string acts as a password to gain access to an SNMP agent. However, neither the frames nor the community string are encrypted. So SNMPv1 and SNMPv2 are not secure. In SNMPv3 can configure Authentication and Privacy is more secure. Setting "add" and "Edit" and "Delete" function for this management





Status						
Network	Gro	up Tabl	е			
ort						
Setting	Show	ving All	 entries 	Showing 0	to 0 of 0 entries	Q [
		1			View	
ess Table		Group	Version	Security Level		Notify
		1		0.00	sults found.	nouly
у				016	First	Previ
	Confi	iqure	to a	issociate a non-de		
	(16)()	oup.
		Add	Edit	Delete		
ווע						
uration SS nent						
nt						
t nt						
;						
n t unt						

Field	Description
Group	Specify SNMP group name, and the maximum length is 30 characters.
-	Spedify SNMP version
	• SNMPv1: SNMP Version 1.
Version	SNMPv2: Community-based SNMP Version 2c.
	• SNMPv3: User security model SNMP version 3.
	Specify SNMP security level
	 No Security : Specify that no packet authentication is performed.
	Authentication: Specify that no packet authentication without encryption
Security Level	performed.
	 Authentication and Privacy: Specify that no packet authentication with
	encryption is performed.
Manajara	Spedify SNMP version
Version	• SNMPv1: SNMP Version 1.





	SNMPv2: Community-based SNMP Version 2c.			
	• SNMPv3: User security model SNMP version 3.			
	Specify SNMP security level			
	 No Security : Specify that no packet authentication is performed. 			
• · · · ·	 Authentication: Specify that no packet authentication without encryption 			
Security Level	performed.			
	 Authentication and Privacy: Specify that no packet authentication with 			
	encryption is performed.			
	Spedify SNMP version			
	Read: Group read view name			
View	Write: Group write view name.			
	 Notify: The view name that sends only traps with contents that is 			
	included in SNMP view selected for notification.			
Read	Group read view name			
Write	Group write view name.			
Notify	The view name that sends only traps with contents that is included in SNMF			
Notify	view selected for notification.			

Group	
Version	SNMPv1 SNMPv2 SNMPv3
	 No Security Authentication Authentication and Privacy
	Read
View	Write all
	Notify
	all 🗸

- Group: Specify SNMP group name, and the maximum length is 30 characters. \succ
- \succ Version: Specify SNMP version.
 - **SNMPv1:** SNMP Version 1.

V1.0a





- **SNMPv2:** Community-based SNMP Version 2c.
- SNMPv3: User security model SNMP version 3.
- \geq Security Level: Specify SNMP security level.
 - **No Security :** Specify that no packet authentication is performed.
 - Authentication: Specify that no packet authentication without encryption is performed.
 - Authentication and Privacy: Specify that no packet authentication with entryption is performed.
- \geq View:
 - Read : Select read view name if Read is checked.
 - Write: Select write view name, if Write is checked.
 - **Notify:** Select notify view name, if Notify is checked.

Click the "Apply" button to save your changes or "Close" the button to close settings.

18.4.3 Community

Communities are only defined in SNMPv1 and v2 because SNMPv3 works with users instead of communities. The users belong to groups that have access rights assigned to them, Setting "add" and "Edit" and "Delete" function for this management.

Management → SNMP → Co	ommunity			
 Network 	Community Tabl	е		
¥ Port				
✤ POE Setting	Showing All 🗸 entri	es Sho	wing 1 to 1 of 1	entries
* VLAN	Community	Group View	Access	
 MAC Address Table 	public	all	Read-Only	
 Spanning Tree 	- pablic		rioud only	First
 Discovery 	The access right of a c	ommunity is de	fined by a grou	
✤ DHCP	Configure		group with a c	
✓ Multicast	Add]	Edit	Delete	
 IP Configuration 			Delete	
 Security 				
* ACL				
¥ QoS				
 Diagnostics 				
– Management				
User Account				
Firmware				
© Configuration				
SNMP View				
Group				
Community				





Field	Description
Community	The SNMP community name. Its maximum length is 20 characters.
	SNMP Community mode.
Community	 Basic: snmp community specifies view and access right.
	 Advanced: snmp community specifies group.
Group	Specify the SNMP group configured by the command SNMP group to define the object available to the community.
View	Specify the SNMP view to define the object available to the community.
	SNMP access mode
Access	Read-Only: Read only.
	Read-Write: Read and write.

Community	
Туре	 Basic Advanced
View	all 🗸
Access	 Read-Only Read-Write
	▼

- **Community:** The SNMP community name. Its maximum length is 20 characters.
- **Type:** Specify SNMP version.
 - Basic: SNMP community specifies view and access right, The access rights of a community can configure with Read Only or Read Write. In addition, Administrator can restrict the access to the community to only certain MIB objects by selecting a view.
 - Advanced: SNMP community specifies group, The access rights of a community are defined by a group. You can configure the group with a specific security model. The access rights of a group are Read, Write, and Notify.
 - View: Specify the SNMP view to define the object available to the community.
- Access: SNMP access mode.
 - Read Only: Read only , Management access is restricted to read-only. Changes cannot be

+(886) 2-8911-6160





made to the community.

- Read Write: Read and write, Management access is read-write. Changes can be made to the switch configuration, but not to the community.
- \succ Group: If set Type for specify SNMP version to "Advanced" type, Must be set specify the SNMP group configured by user to define the object available to the community.

Click the "Apply" button to save your changes or "Close" the button to close settings.

18.4.4 User

An SNMP user is defined by the login credentials (username, passwords, and authentication method) and by the context and scope in which it operates by association with a group and an Engine ID. The configured user has the attributes of its group, having the access privileges configured within the associated view.

Groups enable network managers to assign access rights to a group of users, instead of a single user. A user can only be a member of a single group.

Administrator need to create a SNMPv3 user, a SNMPv3 group must be available, Setting "add" and "Edit" and "Delete" function for this management.

Management → SNMP → U	ser					
⊭ Status						
	User Ta	ble				
Fort						
✤ POE Setting	Showing /	All 🗸 e	entries	Showing	1 to 3 of 3 entries	Q
* VLAN		ser	Group	Security Level	Authentication Method	Privacy Method
MAC Address Table			test2	Authentication	SHA	None
 Spanning Tree 			test2	Authentication	SHA	None
 Discovery 			test	No Security	None	None
* DHCP		iproor .		no occanty	First	Previous 1
 Multicast 	Configure		to a	ssociate an SNMF	v3 group with an SNMPv3	
 IP Configuration 		10		10)	
* Security	Add		Edit	Delete		
* ACL						
¥ QoS						
 Diagnostics 						
– Management						
User Account						
© Firmware						
 Configuration SNMP 						
⊗ SNMP View						
Group						
Community						
User						





Field	Description				
	Specify the SNMP user name on the host that connects to the SNMP agent.				
User	The max character is 30 characters. For the SNMP v1 or v2c, the user name				
	must match the community name				
Group	Specify the SNMP group to which the SNMP user belongs.				
	SNMP privilege mode				
	 No Security : Specify that no packet authentication is performed. 				
	Authentication: Specify that no packet authentication without encryption				
Security Level	is performed.				
	 Authentication and Privacy: Specify that no packet authentication with 				
	encryption is performed.				
	Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy.				
Authentication	None: No authentication required.				
Method	 MD5: Specify the HMAC-MD5-96 authentication protocol. 				
	• SHA: Specify the HMAC-SHA-96 authentication protocol.				
	Encryption Protocol				
Privacy Method	None: No privacy required.				
	DES: DES gorithm				

User	number2
Group	test2 🗸
Security Level	 No Security Authentication Authentication and Privacy
thentication	
Method	O None O MD5 O SHA
Password	1234567890
ivacy	
	None DES



- User: Specify the SNMP user name on the host that connects to the SNMP agent. The max character is 30 characters.
- Security Level: SNMP privilege mode.
 - **No Security:** Specify that no packet authentication is performed.
 - Authentication: Specify that no packet authentication without encryption is performed.
 - Authentication and Privacy: Specify that no packet authentication with encryption is performed.

Authentication

- Method: Authentication Protocol which is available when Privilege Mode is Authentication or Authentication and Privacy.
 - None: No authentication required.
 - **MD5:** Specify the HMAC-MD5-96 authentication protocol.
 - **SHA:** Specify the HMAC-SHA-96 authentication protocol.
- **Password:** The authentication password, The number of character range is 8 to 32 characters.

Privacy

- Method: Encryption Protocol.
 - **None:** No privacy required.
 - **DES:** DES algorithm.
 - **SHA:** Specify the HMAC-SHA-96 authentication protocol.
- **Password:** The privacy password, The number of character range is 8 to 64 characters.

Click the "Apply" button to save your changes or "*Close*" the button to close settings.

18.4.5 Engine ID

The Engine ID is only used by SNMPv3 entities to uniquely identify them. An SNMP agent is considered an authoritative SNMP engine. This means that the agent responds to incoming messages (Get, GetNext, GetBulk, Set), and sends trap messages to a manager. Each SNMP agent maintains local information that is used in SNMPv3 message exchanges. The default SNMP Engine ID is comprised of the enterprise number and the default MAC address. The SNMP Engine ID must be unique for the administrative domain, so that no two devices in a network have the same Engine ID, Setting **"add"** and "Edit" and **"Delete"** function for this management.





Management ⇒ SNMP ⇒ E	ngine ID
* Network	Local Engine ID
✤ Port	User Defined
POE Setting	Engine ID
* VLAN	80006a92038c4dea30dd53 (10 - 64 Hexadecimal Characters)
* MAC Address Table	
 Spanning Tree 	Apply
* Discovery	
* DHCP	Remote Engine ID Table
* Multicast	
 IP Configuration 	Showing All v entries Showing 0 to 0 of 0 entries Q
* Security	Server Address Engine ID
* ACL	0 results found.
* QoS	
 Diagnostics 	First Previous 1
– Management	Add Edit Delete
User Account	
Firmware	
Configuration	
SNMP	
View	
Group	
Community	
User	
Engine ID	

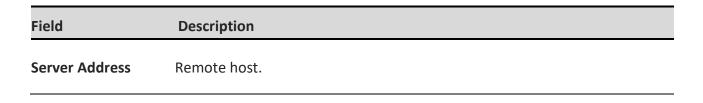
Local Engine ID

Engine ID: If checked "User Defined", the local engine ID is configure by user, else use the default Engine ID which is made up of MAC and Enterprise ID, The user defined engine ID is range 10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

Click the "Apply" button to save your changes settings.

Remote Engine ID Table

Click the "Apply" button to save your changes or "*Close*" the button to close settings.







Engine ID

Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

d Remote Engine Address Type	 Hostname IPv4 	
Server Address	O IPv6	
Engine ID		(10 - 64 Hexadecimal Characters)

- \succ Address Type: Remote host address type for Hostname/IPv4/IPv6.
- Server Address: Remote host. \geq
- \geq Engine ID: Specify Remote SNMP engine ID. The engine ID is range10 to 64 hexadecimal characters, and the hexadecimal number must be divided by 2.

Click the "Apply" button to save your changes or "Close" the button to close settings.

18.4.6 Trap Event

Administrator can choose SNMP Trap Event Type to monitor

Trap messages are generated to report system events, as defined in RFC 1215. The system can generate traps defined in the MIB that it supports.





Status	
Network	Authentication Failure
Port	Link Up / Down 🔽 Enable
POE Setting	
VLAN	Cold Start 🗹 Enable
MAC Address Table	Warm Start 🗹 Enable
Spanning Tree	
Discovery	Apply
DHCP	
Multicast	
IP Configuration	
Security	
ACL	
QoS	
Diagnostics	
• Management	
User Account	
Firmware	
Configuration	
SNMP	
View	
Group	
Community	
User	
Engine ID	
Trap Event	
Notification	

Field	Description
Authentication Failure	SNMP authentication failure trap, when community not match or user authentication password not match.
Link Up/Down	Port link up or down trap
Cold Start	Device reboot configure by user trap
Warm Start	Device reboot by power down trap

Click the "Apply" button to save your changes settings.







18.4.7 Notification

Notification is network nodes where the trap messages are sent by the switch. A list of notification recipients are defined as the targets of trap messages. A trap receiver entry contains the IP address of the node and the SNMP credentials corresponding to the version that will be included in the trap message. When an event arises that requires a trap message to be sent, it is sent to every node listed in the Notification Recipient Table, , Setting **"add"** and "Edit" and **"Delete"** function for this management.

Management → SNMP → N	otification							
 Network 	Notification Table							
✤ Port								
POE Setting	Showing All 🗸 entries		Showin	g 1 to 1 (of 1 entries		(2
* VLAN	Server Address	Server Port	Timeout	Retry	Version	Туре	Community /	User Security Level
MAC Address Table	192.168.2.101	162	THIODUL	nouy	SNMPv1	Trap	public	No Security
Spanning Tree	132.100.2.101	102		_	ONUM VI	map		Previous 1 Next
 Discovery 	For SNMPv1.2 Notification	n	need	s to be d	efined		Filst	Previous II INEXL
* DHCP	For SNMPv3 Notification,		ust be creat		omrou.			
 Multicast 	Add Edi	t)(n	elete					
IP Configuration			elete					
ୡ Security								
¥ ACL								
¥ QoS								
 Diagnostics 								
– Management								
User Account Firmware								
© Configuration								
SNMP								
View								
Group								
Community								
User								
Engine ID Trap Event								
Notification								

Field	Description
Server Address	IP address or the hostname of the SNMP trap recipients.
Server Port	Recipients server UDP port number
Timeout	Specify the SNMP informs timeout
Retry	Specify the retry counter of the SNMP informs.
Version	Specify SNMP notification versionSNMPv1: SNMP Version 1 notification.



	SNMPv2: SNMP Version 2 notification.					
	SNMPv3: SNMP Version 3 notification.					
	Notification Type					
Туре	• Trap: Send SNMP traps to the host.					
	 Inform: Send SNMP informs to the host. 					
Community/User	SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name					
UDP Port	Specify the UDP port number.					
Timeout	Specify the SNMP informs timeout					
	SNMP trap packet security level					
	 No Security: Specify that no packet authentication is performed. 					
Security Level	 Authentication: Specify that no packet authentication without 					
	encryption is performed.					
	 Authentication and Privacy: Specify that no packet authentication with 					

Address Type	 Hostname IPv4 IPv6 	
Comune Addamara	O IPv6	
Server Address	192.168.2.101	
Version	 SNMPv1 SNMPv2 SNMPv3 	
Туре	Trap Inform	
Community / User	public 🗸	
Security Level	No Security Authentication Authentication and F	Privacy
Server Port	Use Default	
Server Port	162	(1 - 65535, default 162)
	💟 Use Default	
	15	Sec (1 - 300, default 15)
	🔽 Use Default	
	3	(1 - 255, default 3)

V1.0a

+(886) 2-8911-6160



- \geq Address Type: Remote host address type for Hostname/IPv4/IPv6.
- \geq Server Address: IP address or the hostname of the SNMP trap recipients.
- \geq Version: Specify SNMP notification version.
 - **SNMPv1:** SNMP Version 1 notification.
 - **SNMPv2:** SNMP Version 2 notification.
 - **SNMPv3:** SNMP Version 3 notification.
- \geq Type: Notification Type.
 - **Trap:** Send SNMP traps to the host.
 - Inform: Send SNMP informs to the host. (version 1 have no inform).
- \geq **Community/User:** SNMP community/user name for notification. If version is SNMPv3 the name is user name, else is community name.
- \geq Security Level: SNMP notification packet security level, the security level must less than or equal to the community/user name.
 - **No Security:** Specify that no packet authentication is performed.
 - Authentication: Specify that no packet authentication without encryption is performed.
 - Authentication and Privacy: Specify that no packet authentication with encryption is performed.
- \geq Server Port: Recipients server UDP port number, if "use default" checked the value is 162, else user configure.
- \geq Timeout: Specify the SNMP informs timeout, if "use default" checked the value is 15, else user configure.
- **Retry:** Specify the SNMP informs retry count, if "use default" checked the value is 3, else user \geq configure.

Click the "Apply" button to save your changes or "Close" the button to close settings.





18.5 **RMON**

18.5.1 **Statistics**

The page displays traffic statistics per interface. The refresh rate of the information can be selected. This page is useful for analyzing the amount of traffic that is both sent and received and its dispersion (Unicast, Multicast, and Broadcast) Click the "Clear" button to clear this page or click the "Refresh" button to refresh and chick the "View" button to view the page .

Status									
Network	Stat	istics	Table						
Port	Defe								
POE Setting	Refre	sh Rate	0 🗸	sec					
VLAN									
MAC Address Table				Bytes	Drop	Packets	Broadcast	Multicast	CRC 8
Spanning Tree		Entry	Port	Received	Events	Received	Packets	Packets	Еп
Discovery		1	GE1	0	0	0	0	0	
ЭНСР		2	GE2	0	0	0	0	0	
lulticast		3	GE3	0	0	0	0	0	
P Configuration		4	GE4	0	0	0	0	0	
curity		5	GE5	0	0	0	0	0	
L		6	GE6	0	0	0	0	0	
s		7	GE7	0	0	0	0	0	
iagnostics		8	GE8	0	0	0	0	0	
lanagement		9	GE9	0	0	0	0	0	
User Account		10	GE10	0	0	0	0	0	
Firmware		11	GE11	0	0	0	0	0	
Configuration		12	GE12	0	0	0	0	0	
RMON		12	GE12	0	0	0	0	0	
			GE13 GE14	0	0	0	0	0	
History		14				-	-	-	
Event		15	GE15	0	0	0	0	0	
Alarm		16	GE16	0	0	0	0	0	

Stati	stics Ta	ble									
efres	h Rate) 💙 se	c								
	Entry	Port	Bytes	Drop	Packets	Broadcast	Multicast	CRC & Align	Undersize	Oversize	Fragments
_			Received	Events	Received	Packets	Packets	Errors	Packets	Packets	riagments
	1	GE1	491071	0	2953	458	545	0	0	0	0
	2	GE2	0	0	0	0	0	0	0	0	0
	3	GE3	0	0	0	0	0	0	0	0	0
	4	GE4	0	0	0	0	0	0	0	0	0
	5	GE5	0	0	0	0	0	0	0	0	0
	6	GE6	0	0	0	0	0	0	0	0	0
	7	GE7	0	0	0	0	0	0	0	0	0
	8	GE8	0	0	0	0	0	0	0	0	C

V1.0a

						Q	
Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
0	0	1215	1044	237	7	442	8
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Field	Description
Port	The port for the RMON statistics.
Bytes Received	Number of octets received, including bad packets and FCS octets, but excluding framing bits.
Drop Events	Number of packets that were dropped.
Packets Received	Number of packets received, including bad packets, Multicast packets, and Broadcast packets.
Broadcast Packets	Number of good Broadcast packets received. This number does not include Multicast packets.
Multicast Packets	Number of good Multicast packets received.
CRC & Align Errors	Number of CRC and Align errors that have occurred.
Undersize Packages	Number of undersized packets (less than 64 octets) received.
Oversize Packages	Number of oversized packets (over 1518 octets) received.
Fragments	Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) eceived.



Jabbers	 Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. A Jabber packet is defined as an Ethernet frame that satisfies the following criteria: Packet data length is greater than MRU. Packet has an invalid CRC. RX error event has not been detected.
Collision	Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.
Frames of 64 Bytes	Number of frames, containing 64 bytes that were received.
Frames of 65 to 127 Bytes	Number of frames, containing 65 to 127 bytes that were received.
Frames of 128 to 255 Bytes	Number of frames, containing 128 to 255 bytes that were received.
Frames of 256 to 511 Bytes	Number of frames, containing 256 to 511 bytes that were received.
Frames of 512 to 1024 Bytes	Number of frames, containing 512 to 1023 bytes that were received.
FramesGreater than 1024 Bytes	Number of frames, containing 1024 to 1518 bytes that were received

18.5.2 History

Use the History Control Table page to define the sampling frequency, amount of samples to store, and the interface from where to gather the data. After the data is sampled and stored, it appears on the History Table page that can be viewed by clicking History Table, , Setting "add" and "Edit" and "Delete" and "View" function for this management.





Status	Liberta and Table
Network	History Table
Port	Showing All 🗸 entries
POE Setting	
VLAN	Sample
MAC Address Table	Entry Port Interval Owner Maximum Current
Spanning Tree	1 GE1 1800 50 50
Discovery	
DHCP	
Multicast	Add Edit Delete View
IP Configuration	
Security	
≱ ACL	
0-0	
¢ Q0S	
Diagnostics	
Diagnostics	
DiagnosticsManagement	
 Diagnostics Management User Account 	
 Diagnostics Management User Account Firmware Configuration SNMP 	
 Diagnostics Management User Account Firmware Configuration SNMP RMON 	
 Diagnostics Management User Account Firmware Configuration SNMP RMON Statistics 	
 Management User Account Firmware Configuration SNMP RMON	
 Diagnostics Management User Account Firmware Configuration SNMP RMON Statistics 	

Field	Description
Port	The port for the RMON history.
Interval	The number of seconds for each sample.
Owner	The owner name of event (0~31 characters).
	The maximum number of buckets.
Sample	• Maximum : The maximum number of buckets.
	Current: The current number of buckets.

V1.0a





Entry	1	
Port	GE1 🗸	
Max Sample	50	(1 - 50, default 50)
Interval	1800	(1 - 3600, default 1800)
Owner		

- \geq **Port:** Select ports for the configure.
- \geq **Max Sample:** Specify the maximum number of buckets.
- Interval: Enter the time in seconds that samples were collected from the interface, Specify the number of seconds for each sample
- Specify the **Owner:** Enter the RMON station or user that requested the RMON information, Specify the owner name of event (0~31 characters).

Click the "Apply" button to save your changes or "Close" the button to close settings.

18.5.3 **Event**

Events page to configure events that are actions performed when an alarm is generated (alarms are defined on the Alarms page). An event can be any combination of logs and traps. If the action includes logging of the events, they are displayed on the Event Log Table page, Setting "add" and "Edit" and "Delete" and "View" function for this management.





Management → RMO Status	
Network	Event Table
Port	
POE Setting	Showing All v entries Showing 0 to 0 of 0 entries Q
VLAN	Entry Community Description Notification Time Owner
MAC Address Table	0 results found.
Spanning Tree	
Discovery	First Previous
DHCP	Add Edit Delete View
Multicast	
IP Configuration	
Security	
ACL	
QoS	
Diagnostics	
- Management	
User Account	
Firmware	
Configuration	
© SNMP	
RMON Statistics	
Statistics	
History Event	
Alarm	

Field	Description
Port	Specify port for the RMON history.
Max Sample	Specify the maximum number of buckets.
Interval	Specify the number of seconds for each sample.
Owner	Specify the owner name of event (0~31 characters).



Entry	1
Notification	 None Event Log Trap Event Log and Trap
Community	Default Community
Description	Default Description
Owner	
Apply	Close

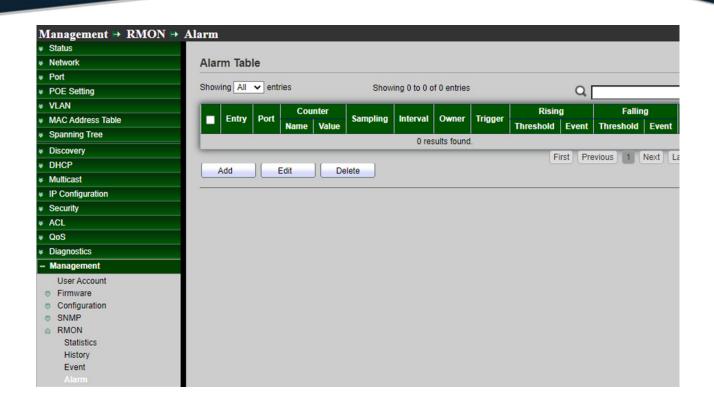
- **Community:** The SNMP community name. Its maximum length is 20 characters. \geq
- \geq **Notification:** Specify the notification type for the event, and the possible value are.
 - **None:** Nothing for notification.
 - **Event Log:** Logging the event in the RMON Event Log table.
 - **Trap:** Send a SNMP trap.
 - Event Log and Trap: Logging the event and send the SNMP trap
- \geq **Community:** Specify the SNMP community when the notification type is specified as "Trap" and "Event Log and Trap".
- **Description:** Specify the description for the event. \geq
- \geq **Owner:** Specify owner for the event.

Click the "Apply" button to save your changes or "Close" the button to close settings.

18.5.4 Alarm

RMON alarms provide a mechanism for setting thresholds and sampling intervals to generate exception events on any counter or any other SNMP object counter maintained by the agent. Both the rising and falling thresholds must be configured in the alarm. After a rising threshold is crossed, no rising events are generated until the companion falling threshold is crossed. After a falling alarm is issued, the next alarm is issued when a rising threshold is crossed, Setting "add" and "Edit" and "Delete" function for this management.





Field	Description
Port	The port configuration for the RMON alarm.
Port	 The port configuration for the RMON alarm. The counter for sampling DropEvents (Drop Event): Total number of events received in which the packets were dropped. Octes (Received Bytes): Octets. Pkts (Received Packets): Number of packets. BroadcastPkts (Broadcast Packets Received): Broadcast packets. MulticastPkts (Multicast Packets Received): Multicast packets. CRCAlignError (CRC and Align Error): CRC alignment error. UndersizePkts (Undersize Packets): Number of oversized packets. OversizePkts (Oversize Packets): Number of oversized packets. Fragments (Fragments): Total number of packet fragment. Jabbers (Jabbers): Total number of packet jabber. Collisions (Collisions): Collision. Pkts64Octetes (Frames of 64 Bytes): Number of packets size 64 octets.
	size 65 to 127 octets.

+(886) 2-8911-6160





	 Pkts128to255Octetes (Frames of 128 to 255 Bytes): Number of
	packets size 128 to 255 octets.
	 Pkts256to511Octetes (Frames of 256 to 511 Bytes): Number of
	packets size 256 to 511 octets.
	 Pkts512to1023Octetes (Frames of 512 to 1023 Bytes): Number of
	packets size 512 to 1023 octets.
	• Pkts1024to1518Octets (Frames Greater than 1024 Bytes): Number of
	packets size 1024 to 1518 octets.
	The sampling type including:
	Absolute: The selected variable value is compared directly with the
	thresholds at the end of the sampling interval
Version	• Delta: The selected variable value of the last sample is subtracted
	from the current value and the difference is compared with the
	thresholds.
Interval	The number of seconds for each sample.
Owner	The owner for the alarm entry.
T (1) (1)	
Trigger	The type of event triggering.
Rising Threshold	The threshold for firing rising event.
Rising Event	The rising event when alarm was fired.
Falling Threshold	The threshold for firing falling event.
Falling Event	The falling event when alarm was fired.

